MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE MOULOUD MAMMERI, TIZI-OUZOU

FACULTE DE GENIE ELECTRIQUE ET DE L'INFORMATIQUE

DEPARTEMENT D'ELECTRONIQUE

Mémoire de fin d'études

En vue de l'obtention

du Diplôme de Master II en Electronique

Option : Réseaux et Télécommunications

Thème :

Implémentation du protocole d'authentification 802.1x avec le serveur RADIUS dans les réseaux informatiques.

Proposé et dirigé par :

Mr. LAHDIR Mourad

Présenté par :

Mlle .MOKRANI Aziza

Mr. BELGHIT Amar

Année universitaire 2010/2011

Remerciements

Nous remercions tout d'abord, notre dieu qui nous a donné la force et le courage pour terminer nos études et élaborer ce modeste travail.

Nous tenons à exprimer nos plus sincères remerciements à notre promoteur Mr.Lahdir, qui nous a aidés tout au long du travail.

Un grand merci à notre Co-promoteur Mr.Kibouh pour et ses orientations qui nous ont beaucoup aidés aux cours de notre projet.

Un grand merci à Mr.Mamou, Mr.Djerman pour les informations qu'ils nous ont donné et leurs encouragements qui nous ont beaucoup servis.

Nous tenons à remercier également nos amis (es) et nos familles pour leurs aides considérables.

Dédicaces

Au nom de dieu miséricordieux

Je dédie ce travail à :

- *Ma très chère mère et à mon père pour leurs précieux aide et soutiens durant tout mon cursus ;*
- *Mes sœurs Faiza, Lila et Amel et mon petit frère Nassim ;*
- *Mes grands parents ;*
- *Mes cousins et cousine, mes oncles et mes tentes et à toute la famille ;*
- *Tous mes amis(es) de oued aissi et hasnaoua et ceux de Bastos et à tous mes amis(es) et camarades de la promotion Master ELN télécommunications 2011 ;*
- *Mes autres amies et camarades du département Electronique promos ingénieurs et licence 2011 ;*
- *Tous ceux qui m'ont aidé ;*
- *Tous ceux que j'aime et à tous ceux qui m'aiment ;*

Amar

Dédicaces

Au nom de dieu miséricordieux

Je dédie ce travail :

A tous ceux qui me sont très chers,

Mes chers parents.

A mes chères sœurs.

A mes chers frères.

A mon cher mari Sofiane.

A mon cher neveu YANIS et son père.

A toute ma famille et ma belle famille sans exception.

A tous mes amis(es), tous ceux qui font partie de ma vie et qui sont chers (es)à mon cœur.

Que dieu nous protège et nous préserve le bonheur et la santé.

Je dédie avec ma profonde affection, ce travail.

AZIZA

Sommaire

ChapitreII : Sécurité des réseaux informatiques

ChapitreIII : L'authentification IEEE 802.1X

Chapitre IV : Le serveur d'authentification RADIUS et l'annuaire Active Diectory.

Chapitre V : Implémentation du protocole d'authentification 802.1x

Introduction générale :

Les réseaux informatiques sont un ensemble d'équipements reliés entre eux pour échanger des informations. Ils ont fait irruption dans le quotidien des entreprises permettant ainsi une amélioration des services qui y sont offerts entre autres le partage de ressources, la gestion centralisée de ces ressources ainsi qu'une meilleure circulation des informations au sein de l'entreprise.

Les réseaux informatiques sont à l'origine de la révolution de la communication et à l'émergence d'une société multimédia. Ils sont la conséquence d'un partage équitable des ressources technologiques. L'information recherchée sur les réseaux de communication doit être localisée très rapidement et dans son intégralité.

Ainsi pour bénéficier des grands avantages que l'interconnexion des réseaux apportent, de plus en plus d'entreprises ouvrent leurs systèmes d'informations a leurs partenaires ou leurs fournisseurs afin de satisfaire leurs besoins en matière d'échange d'information et faire face aux insuffisances de l'utilisation des réseaux locaux en terme de communication. Dans ce cas, lorsque la sécurité d'un réseau est compromise, de très graves conséquences peuvent en résulter, comme l'atteinte à la vie privée, le vol d'informations et même l'engagement de la responsabilité civile et pour rendre cette situation encore plus difficile, les types de menaces potentielles sont en évolution constante.

De plus, la difficulté que représente la sécurité dans son ensemble est de trouver un compromis entre deux besoins essentiels : le besoin d'ouvrir des réseaux pour profiter de nouvelles opportunités commerciales et le besoin de protéger des informations privées ou publiques et des informations stratégiques. Pour cela la sécurité se place actuellement au premier plan de la mise en œuvre et de l'administration réseau.

L'application d'une stratégie de sécurité efficace est l'étape la plus importante qu'une entreprise doit franchir pour protéger son réseau. Faisant partie de cette stratégie de sécurisation, le contrôle de l'accès physique au réseau qui s'avère une opération efficace pour limiter les possibilités d'accès au réseau des entités non désirées.

L'un des moyens pour réaliser ce contrôle est l'authentification des utilisateurs et l'application de droits utilisateurs. Notre objectif dans ce projet est de présenter en détails le protocole 802.1x, dont le but principal est d'autoriser l'accès physique à un réseau local après

une phase d'authentification. Ce protocole s'appuie sur l'encapsulation EAP pour mettre en relation le serveur d'authentification RADIUS et le système à authentifier.

Notre mémoire est organisé en cinq chapitres : Le premier consiste à définir les notions de bases des réseaux informatiques. Le deuxième a pour but d'aborder les notions importantes sur la sécurité des réseaux informatiques. Le troisième chapitre, présente l'authentification IEEE 802.1x, et pour cela nous allons définir la norme 802.1x et les protocoles utilisés par cette dernière telle que EAP, PPP et CHAP. Le quatrième chapitre consiste à définir le protocole RADIUS qui se base principalement sur un serveur RADIUS, relié à une base d'identification (base de données, Annuaire LDAP, Active Directory), Dans le dernier chapitre, nous allons implémenter le protocole 802.1X en configurant les différentes entités le constituant.

Nous terminerons par une conclusion générale en présentant la synthèse de notre travail ainsi que les perspectives et les directions de la recherche.

I.1 INTRODUCTION :

Un réseau est un ensemble d'objets interconnectés les uns avec les autres, il permet de faire circuler des éléments entre chacun de ces objets selon des règles bien définies.
En informatique un réseau est un ensemble d'ordinateurs reliés entre eux grâce à des lignes de connexion physiques et échangeant des informations sous formes de données numériques, c'est-à-dire sous forme de signaux pouvant prendre deux valeurs : 0 et 1.

Il n'existe pas un seul type de réseaux car il existe des type d'ordinateurs différents, communiquant selon des protocoles et langages divers ,de plus les supports physiques de transmission les reliant peuvent être très hétérogènes ,que ce soit au niveau du transfert de données c'est-à-dire circulation des données sous forme de lumière, d'impulsion électrique ou bien d'ondes électromagnétiques ,les réseaux informatiques sont aussi différents au niveau du type du support :lignes en cuivre ,en câble coaxial, en fibre optique …
Dans les parties suivantes du chapitre on va décrire les bases de transmission des données sur le réseau.

I.2 Classification des réseaux :

On distingue différents type de réseaux selon leurs tailles en termes de nombre de machines, leur vitesse de transfert des données ainsi que leurs étendues géographiques …

I. 2.1 selon la topologie géographique on distingue les réseaux suivants :

I.2.1.a Réseau locaux(LAN) :

Un réseau local désigne un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie, la plus répandue étant Ethernet.

I.2.1.b Réseaux métropolitains (MAN) :

Les réseaux métropolitains interconnectent plusieurs réseaux locaux géographiquement proches (au maximum quelques dizaines de kilomètres) avec un débit important. Ainsi un réseau métropolitain permis à deux machines distantes de communiquer comme si elles faisaient partie d'un même réseau local.

Un MAN est formé d'équipements réseau interconnectés par des liens hauts débits qui sont en générale des fibres optiques.

I.2.1.c Réseaux étendue WAN :

Un réseau étendue WAN (Wide Area Network) interconnecte plusieurs réseaux locaux à travers de grandes distances géographiques.

Les WAN fonctionnent grâce à des équipements réseaux appelés routeurs, qui permettent de déterminer le trajet le plus approprié pour atteindre une machine du réseau.

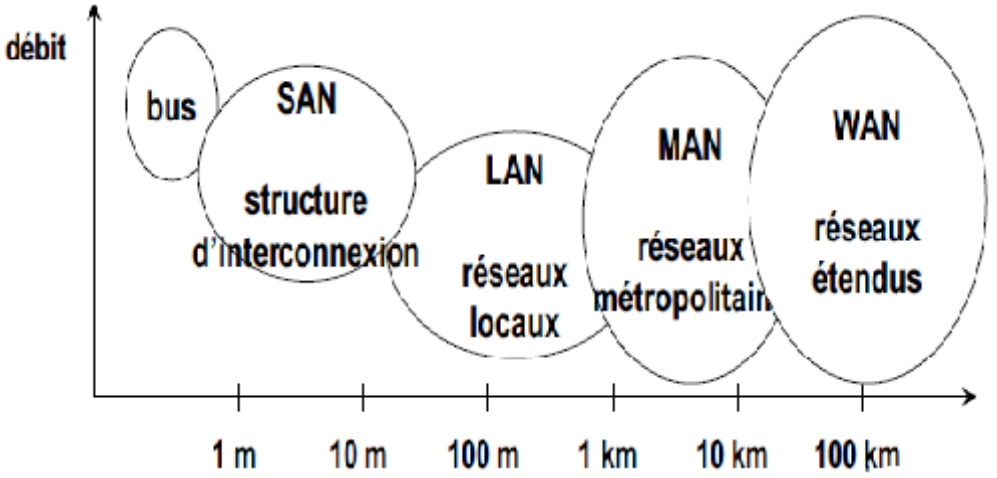


Figure I.1: Les types de réseaux selon l'étendue géographique

I.2.2 selon la topologie physique du réseau :

C'est le classement selon l'arrangement physique, c'est à dire la configuration spatiale du réseau et des machines qui le composent, on distingue généralement les topologies suivantes :

I.2.2.a Topologie en bus :

Tous les équipements sont branchés en série sur le serveur. Chaque poste reçoit l'information mais seul le poste pour lequel le message est adressé traite l'information. On utilise un câble coaxial pour ce type de topologie.

L'avantage du bus est sa simplicité de mise en œuvre et sa bonne immunité aux perturbations électromagnétiques.

Par contre, si le câble est interrompu, toute communication sur le réseau est impossible.

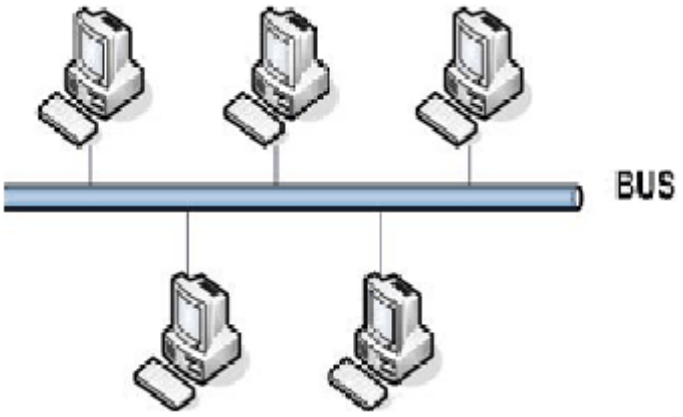


Figure I.2 : Topologie en bus

I.2.2.b Topologie en étoile :

Dans cette topologie, toutes les liaisons sont issues d'un point central (ex : hub). C'est une liaison dite «point à point », c'est à dire que les équipements sont reliés individuellement au nœud central et ne peuvent communiquer qu'à travers lui. On utilise les câbles en paires torsadées ou en fibre optique pour ce type de topologie. L'avantage est que les connexions sont centralisées et facilement modifiables en cas de défectuosité. Si un câble est interrompu, le reste du réseau n'est pas perturbé.

L'inconvénient de taille de cette topologie est l'importante quantité de câbles nécessaire.

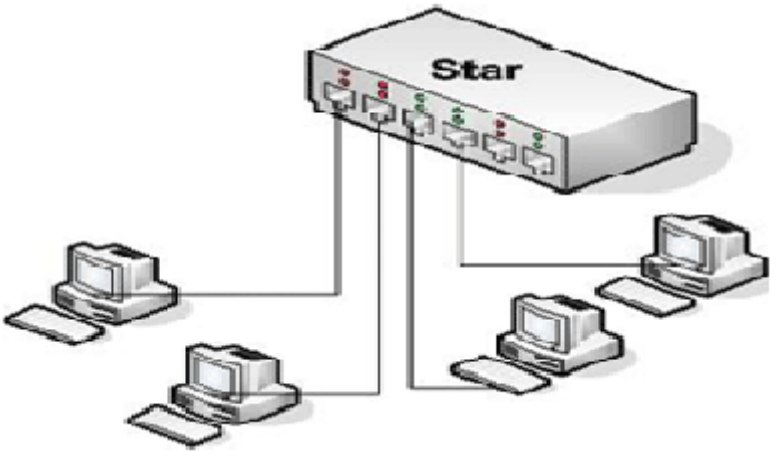


Figure I.3 : Tologie en étoile

I.2.2.c Topologie en anneau :

Les équipements sont reliés entre eux en formant une boucle. La liaison entre chaque équipement est point à point. L'information est gérée comme dans la topologie bus. Chaque station reçoit le message, mais seule la station à qui le message est adressé le traite. Pour le câblage, on utilise un câble en paires torsadées ou de la fibre optique.

L'avantage est que l'anneau offre deux chemins pour aller d'un point à l'autre. Ceci permet à l'information de passer malgré une coupure sur le câble. On utilise cette topologie pour les réseaux de type Token Ring.

Pour augmenter la sécurité, on peut utiliser un double anneau (si le premier anneau est interrompu, les données passent sur l'anneau secondaire, le temps de réparer le premier anneau).

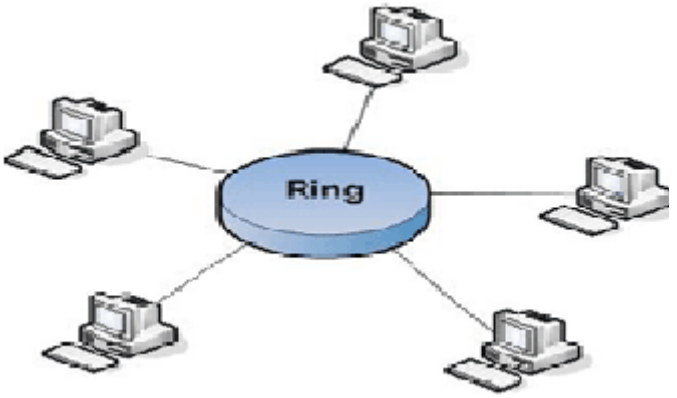


Figure I.4 : Topologie en anneau

I.2.2.d Structure hybride :

La structure hybride de réseau emploie un mélange de différentes structures de réseau, comme l'anneau, le Bus et également l'étoile.

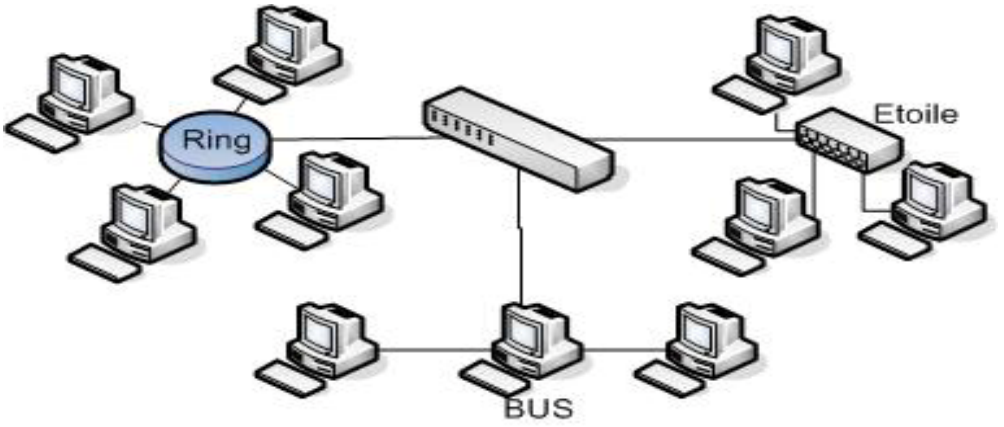


Figure I.5 : Structure hybride

I.3 Architectures réseaux :

En élargissant le contexte de la définition du réseau au service qu'il apporte il est possible de distinguer deux modes de fonctionnement :

I.3.1 Architecture d'égale à égale (Peer to Peer) :

Parfois appelée poste à poste dans cette architecture il n'y a pas d'ordinateur centrale jouant le rôle d'un serveur dédié .Ainsi chaque ordinateur dans un tel réseau est parfois serveur, parfois client .Cela signifie que chacun des ordinateurs du réseau est libre de partager ses ressources.

I.3.1.a Inconvénients des réseaux d'égal à égal :

Les réseaux d'égal à égal ont énormément d'inconvénients :

- ce système n'est pas du tout centralisé, ce qui le rend très difficile à administrer
- la sécurité est très peu présente
- aucun maillon du système n'est fiable

Ainsi, les réseaux d'égal à égal ne sont valables que pour un petit nombre d'ordinateurs (généralement une dizaine), et pour des applications ne nécessitant pas une grande sécurité (il est donc déconseillé pour un réseau professionnel avec des données sensibles).

I.3.1.b Avantages de l'architecture d'égal à égal :

L'architecture d'égal à égal a tout de même quelques avantages parmi lesquels :

- un coût réduit (les coûts engendrés par un tel réseau sont le matériel, les câbles et la maintenance).
- une simplicité à toute épreuve!

I.3.2 Architecture de type client/serveur :

Dans cette architecture un ordinateur serveur fournit des services aux ordinateurs clients.

De nombreuses applications fonctionnent selon un environnement client/serveur, cela signifie que des machines clientes contactent un serveur qui est une machine généralement très puissante en terme de capacité d'entrée-sortie, qui leurs fournit des services .Ces services sont des programmes fournissant des données telles que des fichiers, une connexion…

Les services sont exploités par des programmes, appelés programmes clients, s'exécutant sur les machines clientes. On parle ainsi de client (client FTP, client de Messagerie, etc.) lorsque l'on désigne un programme tournant sur une machine cliente, capable de traiter des informations qu'il récupère auprès d'un serveur (dans le cas du client FTP il s'agit de fichiers, tandis que pour le client de messagerie il s'agit de courrier électronique).

I.3.2.1 Fonctionnement d'un système client/serveur :

Un système client/serveur fonctionne selon le schéma suivant :

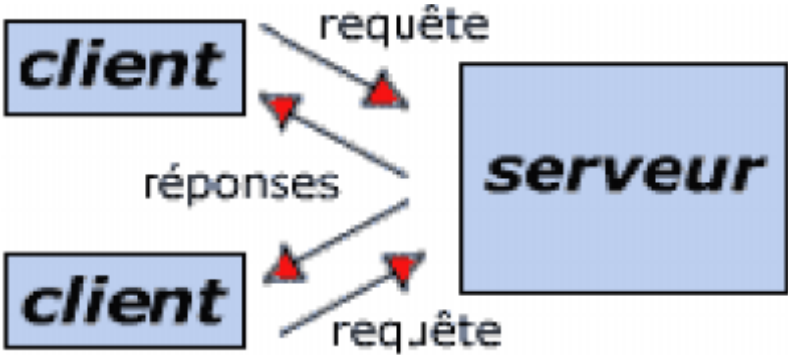


Figure I.6 : Fonctionnement d'un système client /serveur

- Le client émet une requête vers le serveur grâce à son adresse IP et le port, qui désigne un service particulier du serveur
- Le serveur reçoit la demande et répond à l'aide de l'adresse de la machine cliente et son port.

- Notions de bases :

- **Client :** c'est le processus demandant l'exécution d'une opération par l'envoi d'un message contenant le descriptif de l'opération à exécuter et attendant la réponse à cette opération par un message en retour.
- **Serveur :** C'est un processus accomplissant une opération sur demande d'un client.
- **Requête :** C'est un message transmet par un client à un serveur décrivant l'opération à exécuter pour le compte d'un client.
- **Réponse :** C'est un message transmis par un serveur à un client suite à l'exécution d'une opération contenant les paramètres de retour de l'opération.

❖ **Middleware :** C'est un logiciel qui, assure les dialogues entre les clients et les serveurs souvent hétérogènes.

I.3.2.2 Différents types d'architecture client /serveur :

i. L'architecture à deux niveaux :

L'architecture à deux niveaux caractérise les systèmes clients/serveurs pour lesquels le client demande une ressource et le serveur la lui fournit directement (sans intermédiaire), en utilisant ses propres ressources. Cela signifie que le serveur ne fait pas appel à une autre application afin de fournir une partie du service.

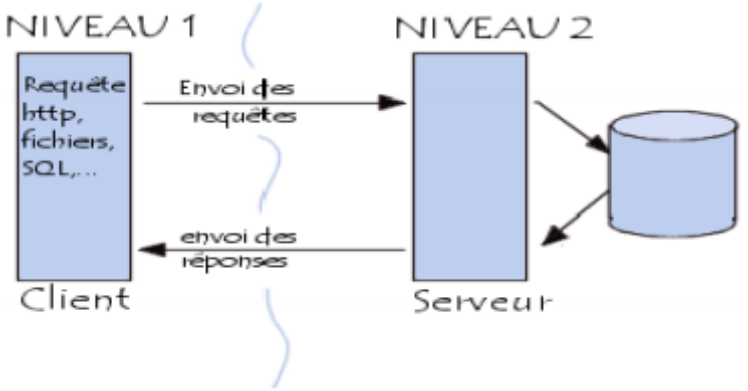


Figure I.7 : Client/serveur à deux niveaux

ii. L'architecture à trois niveaux :

Dans l'architecture à 3 niveaux (appelée *architecture 3-tier*), il existe un niveau intermédiaire, c'est-à-dire que l'on a généralement une architecture partagée entre :

❖ **Un client** : c'est-à-dire l'ordinateur demandeur de ressources.

❖ **Le serveur d'application (appelé également middleware) :** chargé de fournir la ressource mais faisant appel à un autre serveur.

❖ **Le serveur secondaire (serveur de données) :** le serveur fournissant au serveur d'application les données dont il a besoin (souvent un serveur de base de données).

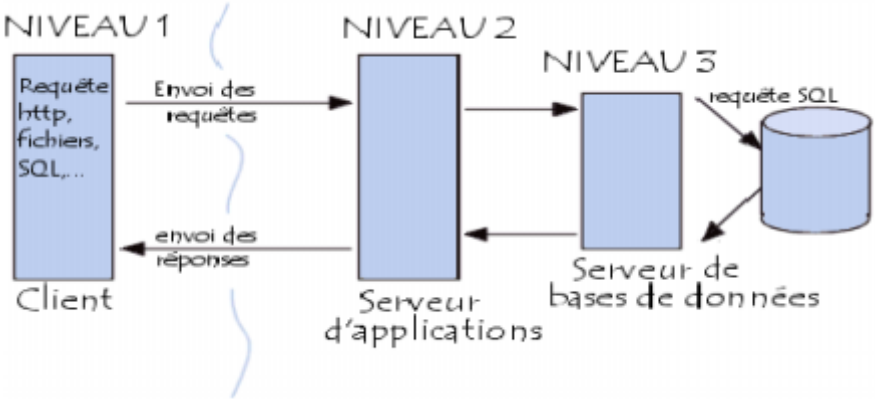


Figure I.8 : Client/serveur à deux niveaux

iii. L'architecture à n niveaux :

L'architecture à n niveaux (n-tiers) a été pensé pour palier aux limitations des architectures trois tiers et concevoir des applications puissantes et simples à maintenir. Ce type d'architecture permet de distribuer plus librement la logique applicative, ce qui facilite la répartition de la charge entre tous les niveaux.

I.3.2.3 Avantages de l'architecture client/serveur :

Le modèle client/serveur est particulièrement recommandé pour des réseaux nécessitant un grand niveau de fiabilité, ses principaux atouts sont :

- **Des ressources centralisées** : étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tous les utilisateurs, comme par exemple une base de données centralisée, afin d'éviter les problèmes de redondance et de contradiction.

- **Une meilleure sécurité** : car le nombre de points d'entrée permettant l'accès aux données est moins important.

- **Une administration au niveau serveur** : les clients ayant peu d'importance dans ce modèle, ils ont moins besoin d'être administrés.

- **Un réseau évolutif** : grâce à cette architecture il est possible de supprimer ou rajouter des clients sans perturber le fonctionnement du réseau et sans modification majeure.

I.3.2.4 Inconvénients du modèle client/serveur :

L'architecture client/serveur a tout de même quelques lacunes parmi lesquelles :

- **Un coût élevé** dû à la technicité du serveur
- **Un maillon faible** : le serveur est le seul maillon faible du réseau client/serveur, étant donné que tout le réseau est architecturé autour de lui ! Heureusement, le serveur a une grande tolérance aux pannes (notamment grâce au système RAID).

I.4 Constituant matériels d'un réseau local :

Un réseau local est constitué d'ordinateurs reliés par un ensemble d'éléments matériels et logiciels .Les éléments matériels permettant d'interconnecter les ordinateurs sont :

- **La carte réseau** : Il s'agit d'une carte connectée sur la carte-mère de l'ordinateur et permettant de l'interfacer au support physique, c'est-à-dire aux lignes physiques permettant de transmettre l'information.

- **Le transceiver :** appelé aussi adaptateur il permet d'assurer la transformation des signaux circulant sur le support physique, en signaux logiques manipulables par la carte réseau, aussi bien à l'émission qu'a la réception.

- **La prise :** il s'agit de l'élément permettant de réaliser la jonction entre la carte réseau et le support physique.

- **Les supports physiques d'interconnexion :** c'est les supports généralement filaires, c'est-à-dire sous forme de câbles, permettant de relier les équipement réseau entre eux, comme les câbles coaxiaux, le câble a paire torsadée et la fibre optique.

I.5 Les équipements d'interconnexion :

Un réseau local sert à interconnecter les ordinateurs d'une organisation, toutefois une organisation généralement plusieurs réseaux locaux, il est donc parfois indispensable de les relier entre eux .Lorsqu'il s'agit de deux réseaux de même type, il suffit de faire passer les trames de l'un sur l'autre .Dans le cas contraire, c'est-à-dire lorsque les deux réseaux utilisent des protocoles différents, il est indispensable de procéder à conversion de protocole avant de transférer les trames.

Ainsi, les équipements à mettre en œuvre sont différents selon la configuration face à la quelle on se trouve .Néanmoins, on retrouve toujours :

I.5.1 Le répéteur :

Il permet d'interconnecter deux segments d'un même réseau. Le répéteur est passif au sens où il ne fait qu'amplifier le signal. Il ne permet pas de connecter deux réseaux de types différents. Il travaille au niveau de la couche 1 du model OSI. Ces fonctions sont :
La répétition des bits d'un segment à l'autre, la régénération du signal pour compenser l'affaiblissement, changer de média (passer d'un câble coaxial à une paire torsadée)

I.5.2 Le pont (bridge) :

Ce sont des équipements qui décodent les adresses machines et qui peuvent donc décider de faire traverser ou non les paquets. Le principe général du pont est de ne pas faire traverser les trames dont l'émetteur et le destinataire sont du même coté, afin d'éviter du trafic inutile sur le réseau.
Il permet d'interconnecter deux réseaux de même type.
Il travaille au niveau de la couche 2 du model OSI.
Il permet aussi de filtrer les trames. Si les stations émettrices et réceptrices se trouvent du même côté du pont, la trame ne le traversera pas pour aller polluer le deuxième segment.

I.5.3 Le concentrateur (HUB) :

C'est un boîtier qui a la fonction de répéteur. Mais sa fonction principale, est de pouvoir concentrer plusieurs lignes en une seule.
On peut y connecter plusieurs stations, dont le nombre dépend du type de HUB.
Un HUB sera connecté sur un autre HUB ou sur un serveur qu'avec une seule et unique ligne.

I.5.4 Le commutateur (Switch) :

Le commutateur (ou Switch) est un système assurant l'interconnexion de stations ou de segments d'un LAN en leur attribuant l'intégralité de la bande passante, à l'inverse du concentrateur qui la partage.

Les commutateurs ont donc été introduits pour augmenter la bande passante globale d'un réseau d'entreprise et sont une évolution des concentrateurs Ethernet (ou hubs).

Ils ne mettent en œuvre aucune fonctionnalité de sécurité (certains commutateurs savent gérer toutefois l'adresse Ethernet (MAC), hormis l'amélioration de la disponibilité. Plusieurs communications simultanées peuvent avoir lieu à condition qu'elles concernent des ports différents du commutateur.

En recevant une information, un Switch décode l'entête pour connaître le destinataire et l'envoie uniquement vers le port Ethernet associé. Ceci réduit le trafic sur l'ensemble du câblage réseau par rapport à un HUB qui renvoie les données sur tous les ports, réduisant la bande passante en provoquant plus de collisions.

A la différence des hubs, La majorité des Switchs peuvent utiliser le mode Full duplex**.** La communication est alors bidirectionnelle, doublant le taux de transfert maximum. Le Switch vérifie automatiquement si le périphérique connecté est compatible full ou half-duplex. Cette fonction est souvent reprise sous le terme "**Auto Négociation.**

I.5.5 Le routeur :

Les routeurs sont les machines clés d'internet car se sont des dispositifs qui permettent de choisir le chemin qu'un message va emprunter .Lorsque nous demandons une URL ,le client web interroge le DNS ,celui-ci indique l'adresse ip de la machine visée .notre poste de travaille envoie la requête au routeur le plus proche (en général la passerelle du réseau) qui choisit la prochaine machine à laquelle il va faire circuler la demande de telle façon que le chemin choisit soit le plus court.

I.5.6 Les passerelles :

Ce sont des systèmes matériels et/ou logiciels permettant de faire des liaisons entre plusieurs réseaux de protocoles différents, l'information est codée et transportée différemment sur chacun de ces réseaux.

Elles permettent aussi de manipuler les données afin de pouvoir assurer le passage d'un type de réseau à un autre. Les réseaux ne peuvent pas faire circuler la même quantité de données simultanément en termes de taille de paquet de données, mais la passerelle réalise cette transition en convertissant les protocoles de communication de l'un vers l'autre.

I.5.7 Les serveurs :

Le serveur est considéré comme le centre d'un réseau. C'est le cerveau du réseau. Il est composé des mêmes sous-ensembles qu'un ordinateur standard. Mais ces sous ensembles sont beaucoup mieux optimisés :

- Il contient plus de mémoire vive
- Son contrôleur de disques est de très bonne qualité (SCSI, voire Wide ou Ultra WideSCSI).
- Disques durs de très grande capacité.
- Microprocesseur(s) de dernière génération.
- Capacités de gestion de réseau.

I.6 Types de serveurs :

Il existe 3 types de serveurs.

- **Serveur de fichier**: s'occupe de la gestion des fichiers. Il faut pour cela un très bon sous-système disque (contrôleur et disques), au moins 32 MB de RAM et une carte réseau très performante.
- **Serveur d'application:** il contient les applications que les utilisateurs du réseau peuvent utiliser. Tous les traitements des logiciels se fait sur le serveur donc la rapidité du microprocesseur et la quantité de RAM (au moins 64MB) sont primordiaux.

- **Serveur d'impression:** c'est lui qui gère les queues d'impression. Ce type de serveur est souvent couplé avec un serveur de fichiers ou un serveur d'applications car il ne demande pas un sous-système très performant.

Il est possible d'installer ces 3 types de serveurs sur la même machine, mais son optimisation devient alors difficile et le risque de pannes augmente.

I. 7 Le model OSI :

OSI signifie (Open System Interconnections), ce modèle a été mis en place par l'ISO (**I**nternational **S**tandard **O**rganisation) afin de mettre en place un standard de communications entre les ordinateurs d'un réseau, c'est-à-dire les règles qui gèrent les communications entre des ordinateurs.

En effet, aux origines des réseaux chaque constructeur avait un système propre (on parle de système propriétaire). Ainsi de nombreux réseaux incompatibles coexistaient.

Le modèle OSI est un modèle qui comporte 7 couches :

I.7.1 Couche physique:

Cette couche définit les propriétés physiques du support de données. Par exemple, dans le cas de câbles en cuivre, les méthodes de transmission sont différentes que celles utilisées sur une liaison par fibre optique. Selon la qualité du support, les vitesses de transmission sont naturellement très variables.

La couche physique est représentée par le matériel de la carte réseau.

I.7.2 Couche Liaison :

La couche liaison assure La fiabilité de la transmission des données par la couche 1, sur le support réseau, Elle réalise cette fonction par l'établissement de sommes de contrôle, par la synchronisation de la transmission des données et par différents procédés d'identification et de correction d'erreurs. L'adressage des ordinateurs est réalisé dans cette couche par les adresses définies de manière fixe sur les cartes réseau. Dans le cas des cartes Ethernet, cette adresse est appelée adresse Ethernet ou adresse matérielle,

La couche liaison est matérialisée et exécutée par un logiciel résidant en ROM sur la carte réseau.

I.7.3 Couche réseau :

Définit l'unité de données de base transférée sur le réseau entre deux sites extrêmes et inclut les concepts d'adressage et de routage.

La couche réseau prend en charge l'optimisation des chemins de transmission entre les ordinateurs distants. Les paquets de données sont transmis grâce à l'établissement d'une connexion logique entre les ordinateurs, qui peut comprendre plusieurs nœuds.

I.7.4 La couche Transport :

La couche transport prend en charge le pilotage du transport des données entre l'expéditeur et le destinataire. Cette fonction est réalisée par les protocoles TCP (Transmission Control Protocol) et UDP (User Datagram Protocol) de la famille des protocoles TCP/IP.

- **TCP :** établit ainsi un protocole orienté connexion pour assurer la transmission des données. Ce type de communication permet de garantir la sécurité de la transmission par une

confirmation de la réception des données par le destinataire. Le protocole attend ainsi un accusé de réception de chaque paquet de données avant de transmettre le paquet suivant. Si l'accusé de réception n'est pas reçu au bout d'un certain temps, le paquet concerné est retransmis au destinataire.

- **UDP :** permet de réaliser la fonction de cette couche par un protocole sans connexion.

Dans ce cas, le destinataire ne transmet pas d'accusé de réception. L'expéditeur ne peut donc pas savoir si les paquets de données ont été correctement reçus par le destinataire. En outre, les checksum sont utilisés de manière moins intensive. S'il est nécessaire de réaliser un traitement des erreurs, celui-ci doit être pris en compte par une couche supérieure du modèle OSI. Cependant, le protocole UDP permet de réaliser un transfert de données plus rapide, en éliminant la nécessité de l'accusé de réception. Ses performances plus importantes justifient sa large utilisation dans le domaine Unix. Pour le service Network File System (NFS).

I.7.5 La couche Session :

Définit la manière dont les protocoles peuvent être organisés pour fournir toutes les fonctionnalités dont les programmes d'applications se servent.
Cette couche gère l'échange des données sur la connexion établie par les couches 1 à 4. En particulier, c'est cette couche qui détermine lequel des ordinateurs connectés doit émettre les données et lequel doit les recevoir.

I.7.6 La couche Présentation :

Est destinée à supporter les fonctions dont beaucoup de programmes ont besoin comme la compression de texte ou la conversion d'image graphique.

I.7.7 La couche application :

Cette couche assure aux processus d'application le moyen d'accès à l'environnement OSI et fournit tout les services directement utilisables par l'application (transfert des données, allocation de ressources, intégrité et cohérence des informations, synchronisation des applications).

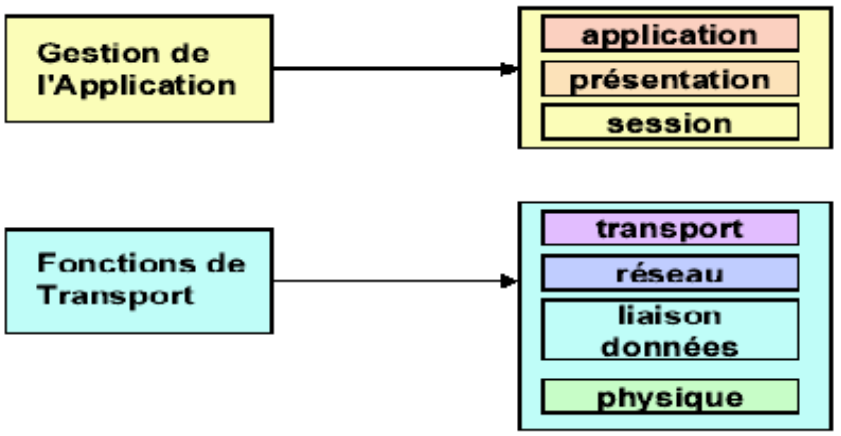


Figure I.8 : Les couches de model OSI

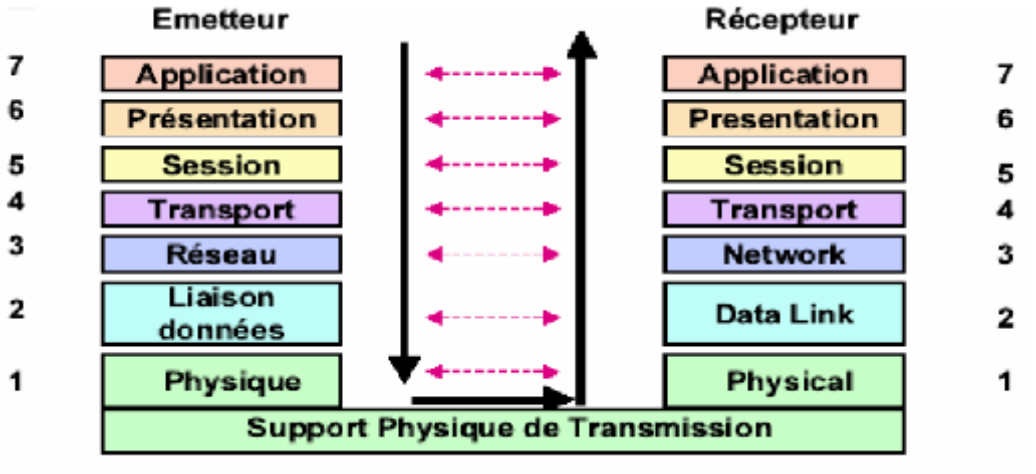


Figure I.9 : model OSI entre émetteur et récepteur

I.8 Le model TCP/IP :

TCP/IP désigne communément une architecture réseau, mais cet acronyme désigne en fait deux protocoles étroitement liés : un protocole de transport, TCP (Transmission Control Protocol) qu'on utilise "par-dessus" un protocole réseau, IP (Internet Protocol). Ce qu'on entend par "modèle TCP/IP", c'est en fait une architecture réseau en quarte couches dans laquelle les protocoles TCP et IP jouent un rôle prédominant, car ils en constituent l'implémentation la plus courante. Par abus de langage, TCP/IP peut donc désigner deux choses : le modèle TCP/IP et la suite de deux protocoles TCP et IP.

I.8.1 Description du modèle :

Le modèle TCP/IP peut en effet être décrit comme une architecture réseau à 4 couches :

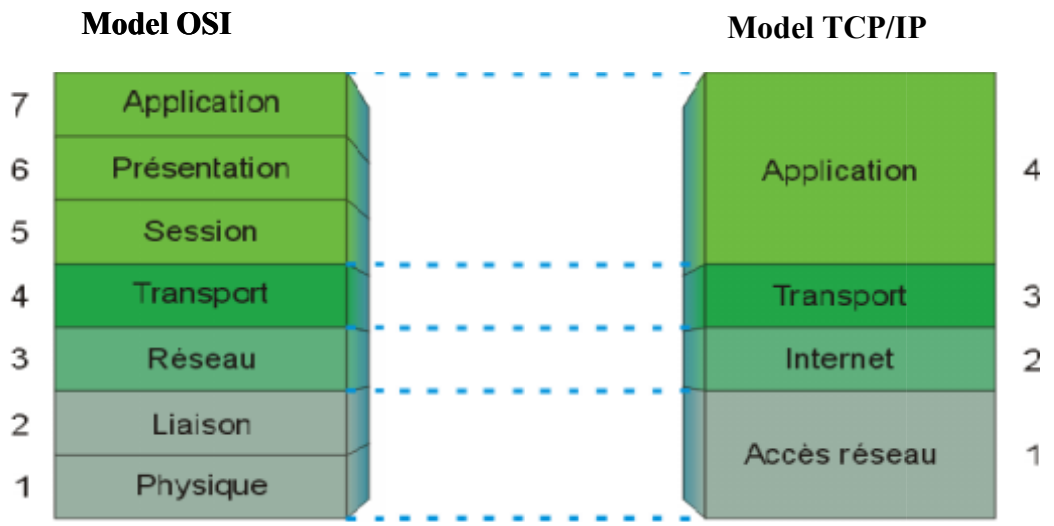


Figure I.9 : Analogie de model OSI avec le model TCP/IP

I.8.1.a La couche application :

C'est la couche située au sommet des couches du protocole TCP/IP .Elle contient les applications réseau permettant de communiquer grâce aux couches inférieures.

I.8.1.b La couche transport :

Elle permet à des applications tournant sur des machines distantes de communiquer.
La couche transport contient deux protocoles permettant à deux applications d'échanger des données indépendamment du type du réseau emprunté (c'est-à-dire indépendamment des couches inferieures …), il s'agit des protocoles suivants :

- TCP : un protocole orienté connexion qui assure le contrôle des erreurs.
- UDP : un protocole non orienté connexion dont le contrôle d'erreur est archaïque.

I.8.1.c La couche internet :

C'est la couche la plus importante, car c'est elle qui définit les datagrammes (paquets de données), et qui gère la notion d'adressage IP.

Elle permet l'acheminement des datagrammes vers des machines distantes ainsi que la gestion de leur fragmentation et de leur assemblage à la réception.
La couche internet contient cinq protocoles : IP, ARP, ICMP, RARP et IGMP.

I.8.1.d La couche accès réseau :

C'est la première couche de la pile TCP/IP, elle offre les capacités à accéder à un réseau physique quel qu'il soit, c'est-à-dire les moyens à mettre en œuvre afin de transmettre des données via un réseau.

Cette couche contient toutes les spécifications concernant la transmission de données sur un réseau physique, qu'il s'agisse de réseau local (Token Ring, Ethernet, FDDI), de connexion à une ligne téléphonique ou n'importe quel type de liaison à un réseau. Elle prend en charge les notions suivantes :

- Acheminement des données sur la liaison.
- Coordination de la transmission de données (synchronisation).
- Format des données.
- Conversion des signaux (analogique /numérique).
- Contrôle des erreurs à l'arrivée.

I.9 Encapsulation des données :

Lors d'une transmission, les données traversent chacune des couches au niveau de la machine émettrice. A chaque couche, une information est ajoutée au paquet de données, il s'agit d'un en-tête, ensemble d'informations qui garantissent la transmission. Au niveau de la machine réceptrice, lors du passage dans chaque couche, l'en-tête est lu, puis supprimé. Ainsi, à la réception, le message est dans son état original.

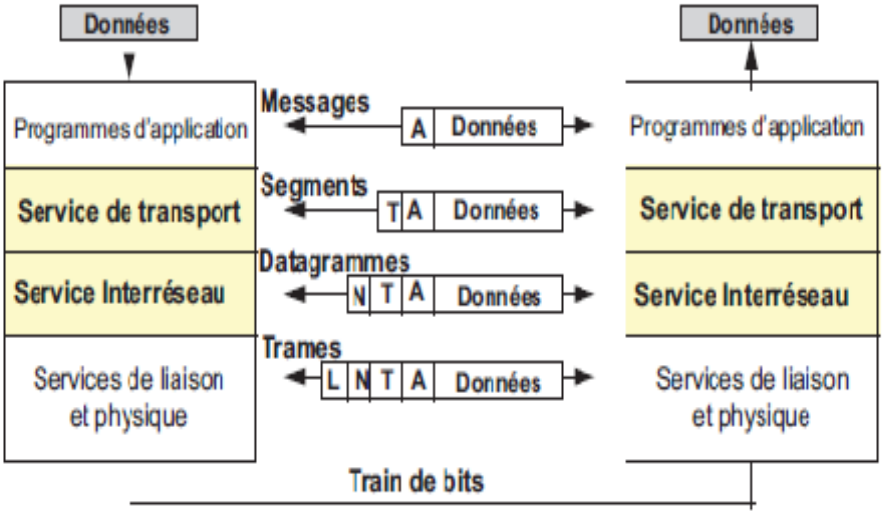


Figure I.11 : Encapsulation au niveau des couches TCP/IP

I.10 L'adressage IP :

L'Internet est donc un réseau basé sur un ensemble de protocoles : les protocoles de la famille TCP/IP. La version actuelle est nommée IPV4 (version 4).

Pour localiser les machines, on fait usage d'adresses. Ces dernières sont utilisées à de nombreux niveaux dans les paquets qui transitent sur le réseau.

Les adresses IP peuvent donc être représentées sur 32 bits. Ces 32 bits sont séparés en deux zones de bits contiguës :

- **Network ID :** une partie décrit le numéro du réseau local auquel est rattachée la station.
- **Host ID :** une partie correspond au numéro de la station dans le réseau local lui-même, appelée numéro d'hôte.

  Selon l'adresse IP on définit différentes classes d'adresses. Il existe cinq classes d'adresses avec la version 4 (version courante) des protocoles TCP/IP, car les parties réseau et hôte n'ont pas toujours la même taille.

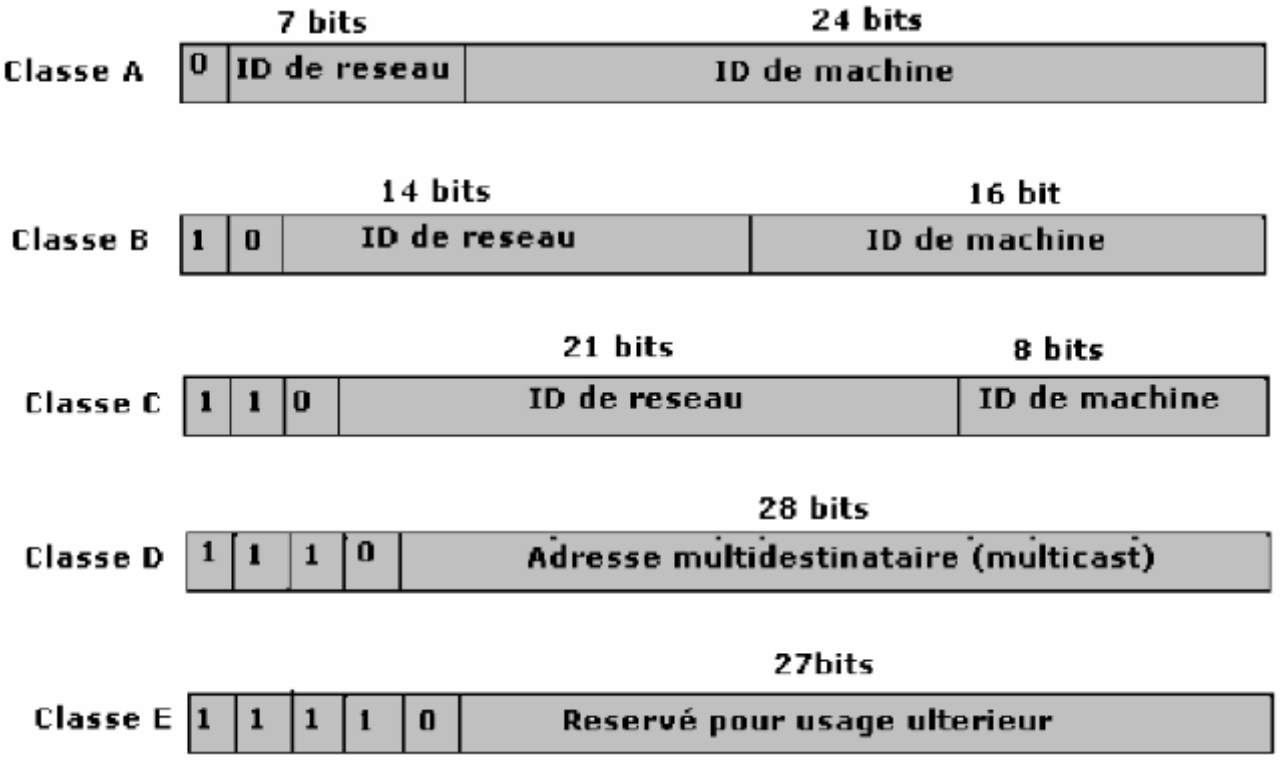


Figure I.12 : Les cinq classes d'adresses IP.

I.11 Conclusion :

La sécurité des réseaux nous impose un bagage plus au moins consistants et des connaissances suffisamment profondes dans les différents types de réseaux (LAN, MAN, WAN), les éléments constituant un réseau, le modèle OSI, le modèle TCP/IP, les différents protocoles de communications entre les équipements du réseau ainsi que des connaissances sur l'architecteur Client/ Serveur sont primordiale pour bien assimiler notre travail.

II. 1Introduction :

La sécurité informatique est de nos jours devenue un problème majeur dans la gestion des réseaux d'entreprise ainsi que pour les particuliers toujours plus nombreux se connecter à Internet. La transmission d'informations sensibles et le désir d'assurer la confidentialité de celles-ci est devenu un point primordiale dans la mise en place de réseaux informatiques, un accès non autorisé ou malveillant aux systèmes informatiques d'une entreprise peut induire en quelques minutes des pertes financières très importantes, la sécurité informatique vise cinq objectifs principales suivants.

Authentification :

C'est l'assurance de l'identité d'un objet, généralement une personne, mais cela aussi s'appliquer à un serveur. Dans la vie courante, la présentation de la carte d'identité et signature manuelle assurent un service d'authentification.

Confidentialité :

C'est l'assurance qu'un document ne sera plus lu par un tiers qui n'en pas le droit c'est-à-dire l'information ne puisse être lue que par les personnes autorisées.

Intégrité :

L'intégrité d'un objet (document, fichier, message) est la garantie que cet objet n'a pas être modifié par une autre personne que par son auteur.

Disponibilité :

Demande que l'information sur le système soit disponible aux personnes autorisées.

Non répudiation :

Elle permet d'assurer qu'un message a bien été envoyé par une source spécifiée et reçu par un récepteur spécifié.

Nous définissons dans ce chapitre la sécurité des réseaux ainsi que les méthodes des attaques utilisées et comment protéger contre elles.

Lorsqu'il est question de sécurité des réseaux, les trois notions qui interviennent habituellement dans la discussion sont la vulnérabilité, les menaces et les attaques.

II.2 Vulnérabilité :

La vulnérabilité est le degré de faiblesse inhérent à tout réseau ou périphérique. Cela concerne les routeurs, les commutateurs, les ordinateurs de bureau, les serveurs et même les périphériques de sécurité.

II.3 Les menaces :

Les menaces viennent d'individus compétents intéressés par l'exploitation des faiblesses de sécurité. Ces menaces sont mises en œuvre à l'aide d'une variété d'outils, de scripts et de programmes permettant de lancer des attaques contre des réseaux et leurs périphériques. En général, les périphériques réseau attaqués sont des points d'extrémité comme les serveurs et les ordinateurs de bureau.

Il existe cinq catégories de menaces : divulgation, interruption, modification, destruction et enlèvement.

II.4 Les failles de sécurité sur Internet :

En entreprise, c'est le réseau local qui est connecté à Internet. Il est donc indispensable de contrôler les communications entre le réseau interne et l'extérieur. De plus une formation du personnel est indispensable (règles de sécurité, déontologie, attention aux participations aux forums qui sont archivées ...).

Les problèmes de sécurité qu'on peut rencontrer sur un réseau d'entreprise ou sur l'Internet relèvent d'abord de la responsabilité des victimes avant d'être imputables aux hackers.

D'autre part, votre sécurité peut dépendre d'autres entreprises dont vous pensez, parfois à tort, qu'elles ont assuré leur propre sécurité. Alors que le gouvernement et les forces de l'ordre cherchent à interpeller les intrus, les sociétés ne se préoccupent trop souvent que de relancer leurs réseaux après une attaque. « Le secteur privé ne cherche pas à savoir qui est responsable, tout ce qui intéresse les entreprises, c'est que l'attaque cesse. ».

II.4.1 Les pirates :

Le terme de pirate englobe toutes les personnes qui enfreignent les lois de l'informatique. Ces lois sont établies par chaque pays, cela pose un problème car Internet est accessible à tous les habitants de la planète et certains actes sont des infractions pour les uns mais pas obligatoirement pour les autres. Le pirate est une personne qui viole les droits d'autrui ou des sociétés à son profit. Les pirates les plus communs sont les hackers, les

crackers et toute personne copiant du software pour son utilisation personnelle ou pour la vente.

II.4.2 Les hackers et les crackers:

Il existe une communauté, une culture partagée, de programmeurs expérimentés et de spécialistes des réseaux, dont l'histoire remonte aux premiers mini-ordinateurs multiutilisateurs, il y a quelques dizaines d'années. Les membres de cette culture ont créé le mot **"hacker''.** Ces informaticiens sont généralement discrets, anti-autoritaristes et motivés par la curiosité.

Il y a un autre groupe de personnes qui s'autoproclament des "hackers". Ces gens prennent leur pied en s'introduisant à distance dans les systèmes informatiques et en piratant les systèmes téléphoniques, généralement à l'aide d'outils écrit par d'autres et trouvés sur Internet. Les vrais hackers appellent ces gens des **"crackers"** et ne veulent rien avoir à faire avec eux. Les vrais hackers pensent que les crackers sont des gens paresseux, irresponsables et pas très brillants.

II.4.3 Les attaques :

Parmi les types d'attaques du réseau on distingue :

II.4.3.1 Virus :

Les virus représentent la menace sur la sécurité la plus largement connue. Les virus sont des programmes informatiques exécutables écrits par des programmeurs mal intentionnés et conçu. Ils se chargent dans la mémoire vive de l'ordinateur afin d'infecter les fichiers exécutables lancés par l'utilisateur. Les effets de certains virus sont plus destructifs et peuvent supprimer des fichiers d'un disque dur ou ralentir un système.

II.4.3.2 Ver :

Un ver est un programme qui peut se reproduire et se déplacer à travers un réseau en utilisant ses mécanismes, sans avoir réellement besoin d'un support physique ou logique (disque dur, fichier…) pour se propager, donc un ver est un virus réseau. Voici la façon dont le ver se propagerait sur le réseau :

- Il s'introduisait sur une machine de type Unix
- Il dressait une liste des machines qui lui étaient connectées
- Il forçait les mots de passe à partir d'une liste de mots
- Il se faisait passer pour un utilisateur auprès des autres machines

- Il créait un petit programme sur la machine pour pouvoir se reproduire

II.4.3.3 Cheval de Troie :

Un cheval de Troie est un programme qui se cache lui-même dans un autre Programme apparemment au-dessus de tout soupçon. Quand la victime lance ce programme, elle lance par-là même le cheval de Troie caché. Actuellement, les chevaux de Troie les plus utilisés sont : Back Orifice 2000, Netbios, Socket de Troie….

La méthode la plus efficace pour se protéger de ces programmes est d'utiliser un bon antivirus.

II.4.3.4 Déni de service (DoS) :

Le but d'une telle attaque est de paralyser un service ou un réseau complet. Les utilisateurs ne peuvent plus alors accéder aux ressources.

II.4.3.5 Attaque man in the middle:

Une attaque man in the middle (attaque de l'homme de milieu) est un scénario d'attaque avec lequel un pirate écoute ou modifie une communication entre deux interlocuteurs.

I.4.3.6 Ecoute du réseau (Sniffer) :

Est un dispositif logiciel permettant d'écouter le trafic d'un réseau, c'est-à-dire de capturer les informations qui y circulent sur ce réseau. Le sniffer peut ainsi servir à déceler les failles de sécurité, mais il peut aussi être utilisé de façon malveillante (pour intercepter les mots de passe du réseau par exemple).

I.4.3.7 Intrusion :

L'intrusion dans un système informatique a généralement pour but la réalisation d'une menace donc une attaque. Les conséquences peuvent être catastrophiques : vol, fraude, chantage.

I.4.3.8 Espiogiciels (spyware) :

Est un programme chargé de recueillir des informations sur l'utilisateur de l'ordinateur dans lequel il est installé afin de les envoyer vers la société qui le diffuse pour lui permettre de dresser le profil des internautes.les récoltes des informations peuvent être les adresses WEB

des sites visités, les mots clés saisis dans les moteurs de recherche, des informations personnelles, etc.

I.4.3.9 Objectifs des attaques :

- Désinformer
- Empêcher l'accès à une ressource
- Prendre le contrôle d'une ressource
- Récupérer de l'information présente sur le système
- Utiliser le système compromis pour rebondir
- Constituer un réseau de « botnet » (ou réseau de machines zombies)

I.5 Les méthodes de sécurité :

I.5.1 Mise en place d'une politique de sécurité :

La politique de sécurité est un ensemble de règles qui fixent les actions autorisées et interdites dans le domaine de sécurité.

I.5.1.a En quoi consiste une politique de sécurité :

La politique mise en œuvre doit contrôler les accès à des zones définies du réseau et comment interdire l'accès à certaines zones à des utilisateurs non autorisés. Par exemple, seuls les membres du service des ressources humaines doivent avoir accès à l'historique des salaires des employés. Les mots de passe empêchent généralement les employés d'accéder aux zones protégées, mais à la condition que ceux-ci demeurent confidentiels. Des politiques écrites stipulant par exemple, que les employés ne doivent pas afficher leurs mots de passe sur leur bureau peuvent souvent prévenir certaines failles dans la sécurité.

Les clients ou fournisseurs ayant accès à certaines parties du réseau doivent également être l'objet de règles adéquates de ces politiques.

II.5.1.b Qui doit appliquer et gérer cette politique :

La personne ou le groupe chargé de gérer et d'entretenir le réseau et sa sécurité doivent avoir accès à toutes ses zones. La fonction de gestion des politiques de sécurité doit donc être confiée à des personnes particulièrement dignes de confiance et disposant des compétences techniques nécessaires.

Ainsi que nous l'avons mentionné auparavant, la plupart des failles dans la sécurité proviennent de l'intérieur, cette personne ou ce groupe ne doit donc pas constituer une menace potentielle. Une fois désignés, les gestionnaires du réseau bénéficient d'outils logiciels sophistiqués leur permettant de définir, de distribuer, de renforcer et d'évaluer les politiques de sécurité au moyen d'interfaces utilisant le modèle d'un navigateur Internet.

II.5.2 Comment protéger un réseau ?

II.5.2.1 L'antivirus :

Principale cause de désagrément en entreprise, les virus peuvent être combattu à plusieurs niveaux.

La plus part des ordinateurs sont dotés d'un logiciel antivirus préintégré capable de détecter les principales menaces virales s'il est régulièrement mis à jour.

Avec des milliers de nouveau virus gérés chaque mois il est essentiel que la base des données des virus soit tenue à jour. La base des données des virus et l'enregistrement de logiciel antivirus qui permet d'identifier les virus connus lorsqu'ils surviennent.

II.5.2.1.1 On distingue deux méthodes de protections :

- Soit sur le poste de travail de l'utilisateur et là l'antivirus servira généralement inspecter et désinfecter le disque dur, il faut absolument prévoir une mise à jour automatique de tous les postes.
- Soit à l'entrée d'un réseau local, là ou arrivent les flux en provenance de l'Internet ; certains de ces flux seront filtrés pour détecter des virus, essentiellement les flux relatifs aux protocoles SMTP (courrier électronique) et http (WEB).

II.5.2.2 Cryptage et Authentification :

II.5.2.2.a Définition :

La cryptographie est une méthode permettant de rendre secrètes (illisibles) des informations afin de garantir l'accès à un seul destinataire authentifié. Elle est essentiellement basée sur l'arithmétique : il s'agit de transformer les lettres qui composent le message en succession de chiffres (sous forme des bits dans le cas de l'informatique), puis faire des calculs sur ces chiffres pour :

- D'une part les modifier de telle façon à les rendre incompréhensible.
- Faire en sorte que le destinataire saura les décryptées.

Le fait de coder un message de façon à le rendre secret s'appelle le cryptage. La méthode inverse est appelée décryptage, elle nécessite une clé de décryptage.

On distingue de types de cryptages :

II.5.2.2.b Cryptage symétrique :

Le cryptage symétrique appelé également cryptage à clé secrète ou chiffrement conventionnel, utilise une même clé pour crypter et décrypter le message, très efficace et assez économe en ressource CUP. Les algorithmes de chiffrement les plus connus sont :

DES (Data Encryption Standard) et 3DES et AES.

Le principe problème de cette technique la distribution des clés dans un réseau étendu, nécessite de partager une seul clé avec chacun de nos correspondants.

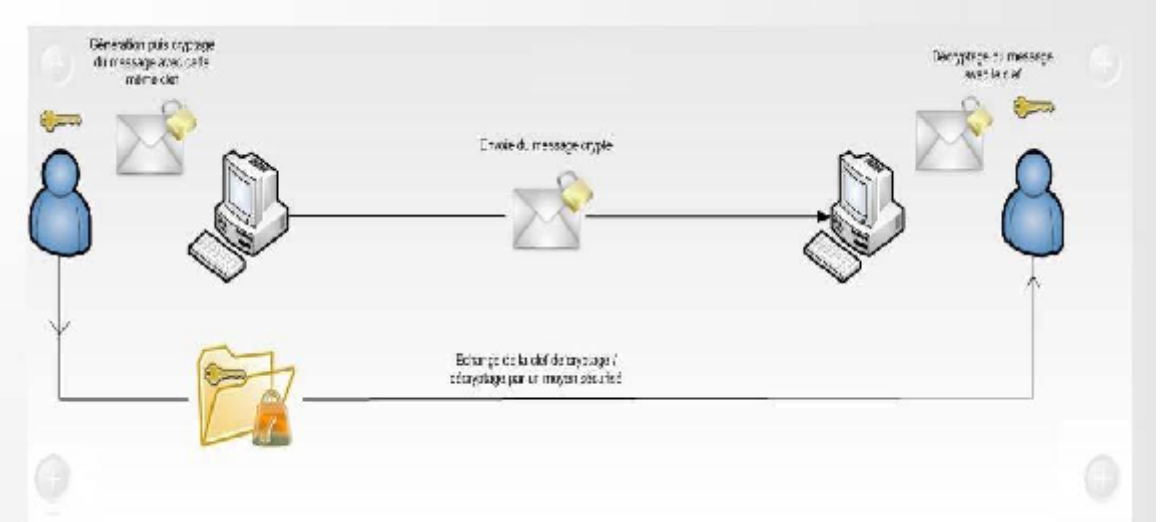


Figure II.1 : cryptage symétrique

II.5.2.2.c Cryptage asymétrique :

Ce système de cryptage utilise deux clés différentes pour chaque utilisateur : une est privée et n'est connue que par son propriétaire ; l'autre est publique et donc accessible par tout le monde.

Les clés publique et privée sont mathématiquement liées par l'algorithme de cryptage de telle manière qu'un message crypté avec une clé publique ne puisse être décrypté qu'avec la clé privée correspondante car ces deux clés générer au même temps. Une clé est donc utilisée pour le cryptage et l'autre pour le décryptage.

Le principal avantage du cryptage à clé publique est de résoudre le problème de l'envoi de clé privée sur un réseau non sécurisé. Bien que plus lent que la plupart des cryptages à clé privée il reste préférable pour 3 raisons :

- Plus évolutif pour les systèmes possédant des millions d'utilisateurs

- Permet de signer le message donc garantir l'Authentification et la non répudiation.
- Supporte les signatures numériques.

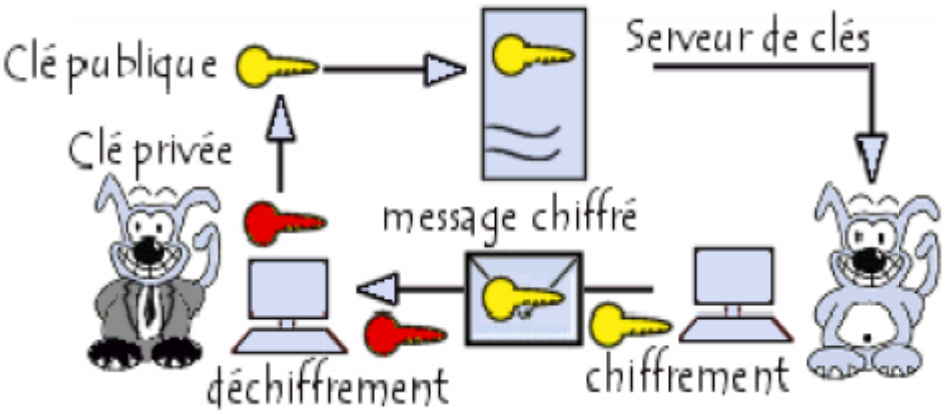


Figure II.2 : cryptage asymétrique

II.5.2.2.d : les fonctions de hachage :

i : Définition :

Une fonction de hachage est très utilisée en cryptographie, principalement dans le but de réduire la taille des données à traiter par la fonction de cryptage. En effet, la caractéristique principale d'une fonction de hachage est de produire un haché des données, c'est-à-dire un condensé de ces données. Ce condensé est de taille fixe, dont la valeur diffère suivant la fonction utilisée.

Le but de condensé est simple : représenter des données de façon certaine tout en réduisant la taille utile qui sera réellement chiffrée

ii: Fonctions de hachage usuelles :

- **MD5** produit des hachés de 128 bits en travaillant les données originales par blocs de 512 bits.
- **SHA-1** (Secure Hach Algorithm 1), comme MD5, il fonctionne également à partir de blocs de 512 données et produit par contre des condensées de 160 bits en sortie. Il nécessite donc plus de ressources que MD5.
- **SHA-2** (Secure Hach Algorithm 2), a été publié récemment et est destiné à remplacer SHA-1. Les différences principales résident dans les tailles de hachés possibles : 256,384ou 512 bits. Il sera bientôt la nouvelle référence en termes de fonction de hachage.

II.5.2.3 L'authentification :

II.5.2.3.a Définition :

Permettant de vérifier les identités présumées des utilisateurs. Lorsqu'il existe une seule preuve de l'identité (mot de passe par exemple) on parle de l'authentification simple. Lorsque nécessite plusieurs facteurs on parle de l'authentification forte. L'authentification permet de vérifier l'identité d'un utilisateur sur une des bases suivantes :

- Un élément d'information que l'utilisateur connaît (mot de passe, ect)
- Un élément que l'utilisateur possède (carte à puce, clé de stockage, certificat)
- Une caractéristique physique propre à l'utilisateur, on parle alors de biométrie (ADN, empreinte digitale, fond de rétine.).

II.5.2.3.b Les différentes méthodes utilisées pour l'authentification :

❖ **Les clés :**

Une clé est une valeur qui est utilisée avec un algorithme cryptographie pour produire un texte chiffré spécifique, sa taille se mesure en bits. Plus la clé est grande, plus le chiffrement est sûr.

❖ **Certificat numérique :**

1. **Présentation :**

Un certificat numérique (aussi appelé certificat électronique) est un fichier permettant de certifier l'identité du propriétaire d'une clé publique, un peu à la manière d'une carte d'identité. Un certificat est généré dans une infrastructure à clés publiques (aussi appelé **PKI** pour **Public Key Infrastructure**) par une autorité de certification (Certification Authority, CA) qui a donc la capacité de générer des certificats numériques contenant la clé publique en question.

Actuellement, les certificats numériques sont reconnus à la norme **X.509 version 3**. Ce format se compose entre autre de :

- X.509 (actuellement la V3).
- Le numéro de série.
- L'algorithme de signature.
- Le nom de l'émetteur (autorité de certification).
- La date de début de fin de validité.
- L'adresse électronique du propriétaire.
- La clé publique à transmettre.
- Le type de certificat.

- l'empreinte du certificat (signature électronique).

La signature électronique est générée par l'autorité de certification à l'aide d'informations personnelles (telles que le nom, le prénom, l'adresse e-mail, le pays du demandeur, etc) en utilisant sa propre clé privée.

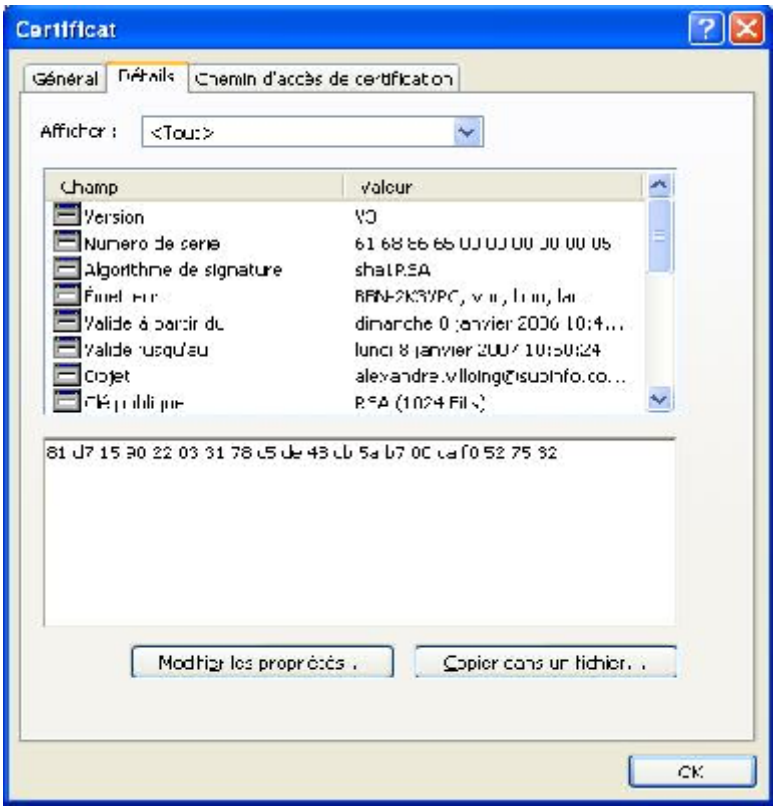


Figure II.3 : Exemple d'un certificat numérique

Il existe de nombreux types de certificats numériques, répondant chacun à un besoin particulier. Les principaux types sont :

- Certificat de messagerie (permet de crypter et de signer ses e-mails).
- Authentification IP Sec pour un accès distant par VPN.
- Authentification Internet pour les pages Web sécurisées.
- Cryptage des données avec EFS.
- Signature de logiciel.

2. Le rôle d'un certificat numérique:

Un certificat numérique intervient dans différents mécanismes permettant de sécuriser l'échange de données sur un réseau. On y retrouve le cryptage asymétrique ou encore la signature électronique combinée à un contrôle d'intégrité des données.

3. Utilisation d'un certificat numérique pour sécuriser le cryptage asymétrique :

Un certificat numérique permet, lors d'un cryptage asymétrique, de garantir lorsque cela s'avère nécessaire, l'identité des différents intervenants. Prenons l'exemple de l'envoi d'un message crypté de manière asymétrique entre deux utilisateurs.

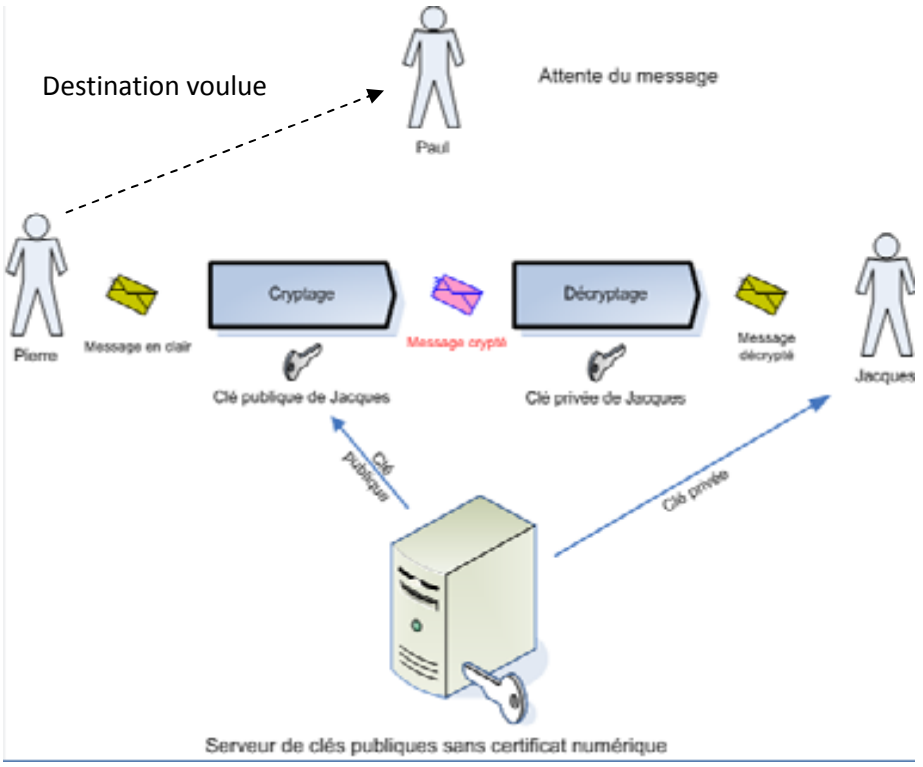


Figure II.4 : Utilisation d'un certificat numérique pour sécuriser le cryptage

Dans ce cas, Pierre veut transmettre des informations confidentielles à Paul. Il va donc récupérer auprès du serveur de clés publiques la clé de cryptage qu'il pense être celle de Paul. Malheureusement, sans certificat (donc sans carte d'identité) l'identité du propriétaire de la clé publique n'est pas garantie. Pierre va donc crypter le message avec la clé publique qu'il pensera être celle de Paul mais qui appartiendra en réalité à Jacques le pirate. Jacques n'aura donc plus qu'à récupérer le message et pourra le décrypter sans aucun problème avec sa propre clé privée.

Dans le cas de l'utilisation d'un certificat numérique, Pierre se serait aperçu que la clé publique ne pouvait pas appartenir à Paul et n'aurait donc pas transmis son message.

4. Signature numérique et la non-répudiation des données :

4.1 Le rôle d'une signature numérique et de la non-répudiation de données :

Alors que le cryptage permet d'empêcher une personne non autorisée à accéder à un contenu protégé, la signature numérique est un procédé qui permet de s'assurer que l'émetteur d'un message est bien celui qu'il prétend être.

5. Les infrastructures à clés publiques (PKI) :

Une PKI (Public Key Infrastructure), aussi appelée IGC (Infrastructure de Gestion de Clés) est une infrastructure réseau qui a pour but final de sécuriser les échanges entre les différents composants d'un réseau.

Cette infrastructure se compose de quatre éléments essentiels :

5.1 L'autorité d'enregistrement (Registration Authorities) :

C'est cette autorité qui aura pour mission de traiter les demandes de certificat émanant des utilisateurs et de générer les couples de clés nécessaires (clé publique et clé privée). Son rôle peut s'apparenter à la préfecture lors d'une demande de carte d'identité.

5.2 L'autorité de Certification (Certification Authorities) :

Elle reçoit de l'Autorité d'Enregistrement les demandes de certificats accompagnées de la clé publique à certifier. Elle va **signer à l'aide de sa clé privée** les certificats, un peu à la manière de la signature de l'autorité sur une carte d'identité. Il s'agit du composant le plus critique de cette infrastructure en raison du degré de sécurité requis par sa clé privée.

5.3 L'autorité de Dépôt (PKI Repositories) :

Il s'agit de l'élément chargé de diffuser les certificats numériques signés par la CA sur le réseau (privé, Internet, etc).

5.4 Les utilisateurs de la PKI :

Ce sont les personnes effectuant des demandes de certificat mais aussi ceux qui souhaitent vérifier l'identité d'un certificat qu'ils ont reçu.

6. Types d'autorités de certification :

Il existe deux types principaux d'installation pour l'autorité de certification :

6.1 Autorité d'entreprise :

Elle est utilisée si l'autorité de certification doit délivrer des certificats dans un domaine auquel appartient le serveur (se base sur l'annuaire d'Active Directory). Cette autorité doit-être contrôleur de domaine.

6.2 Autorité autonome :

Permet de délivrer des certificats dans un réseau comme Internet. Il existe deux niveaux fonctionnels pour chacun de ces deux types d'installation pour l'autorité de certificat :

- **Autorité racine :** Cette autorité de certification est la première du réseau.
- **Autorité secondaire :** dépend d'une autorité racine.

❖ **Signature numérique :**

Signature reposant sur un système de chiffrement à clé publique et à clé privée permettant d'authentifier l'émetteur d'un document électronique. La clé privée sert à signer et la clé publique sert à vérifier cette signature. Les principales avantages elle n'est pas répudiable, protection contre les modifications, signer directement tout ce qui est numérisation. Le seul inconvénient c'est une procédure complexe.

II.5.2.4 Les dispositifs de sécurité :

II.5.2.4.a Firewall (Pare- feu):

C'est un ensemble de différents composants matériels et logiciels qui contrôlent le trafic intérieur / extérieur selon une politique de sécurité. Un pare-feu (appelé aussi coupe-feu, garde-barrière ou firewall en anglais), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :

- une interface pour le réseau à protéger (réseau interne).
- une interface pour le réseau externe.

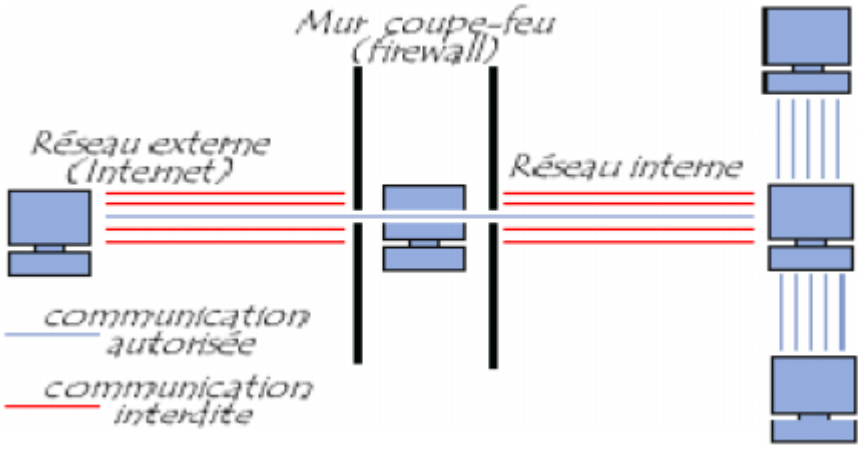


Figure II.4 Firewall

Le système firewall est un système logiciel, reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre le réseau local (ou la machine locale) et un ou plusieurs réseaux externes. Il est possible de mettre un système pare-feu sur n'importe quelle machine et avec n'importe quel système pourvu que :

- La machine soit suffisamment puissante pour traiter le trafic
- Le système soit sécurisé ;
- Aucun autre service que le service de filtrage de paquets ne fonctionne sur le serveur.

❖ **Fonctionnement d'un système pare feu :**

Un système pare-feu contient un ensemble de règles prédéfinies permettant :

- D'autoriser la connexion (allow).
- De bloquer la connexion (deny).
- De rejeter la demande de connexion sans avertir l'émetteur (*drop*).

II.5.2.4.b Serveur mandataire (proxy) :

Un serveur proxy (traduction en français de proxy server, appelé aussi serveur mandataire) est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local (utilisant parfois des protocoles autres que le protocole TCP/IP) et Internet.

La plus part de temps le serveur proxy est utilisé pour le Web, il s'agit alors d'un protocole http. Toutefois il peut exister des serveurs proxy pour chaque protocole applicatif (FTP, etc).

❖ **Le principe de fonctionnement d'un proxy :**

Le principe de fonctionnement basique d'un serveur proxy est assez simple : il s'agit d'un serveur "mandaté" par une application pour effectuer une requête sur Internet à sa place. Ainsi, lorsqu'un utilisateur se connecte à internet à l'aide d'une application cliente configurée pour utiliser un serveur proxy, celle-ci va se connecter en premier lieu au serveur proxy et lui donner sa requête. Le serveur proxy va alors se connecter au serveur que l'application cliente cherche à joindre et lui transmettre la requête. Le serveur va ensuite donner sa réponse au proxy, qui va à son tour la transmettre à l'application cliente.

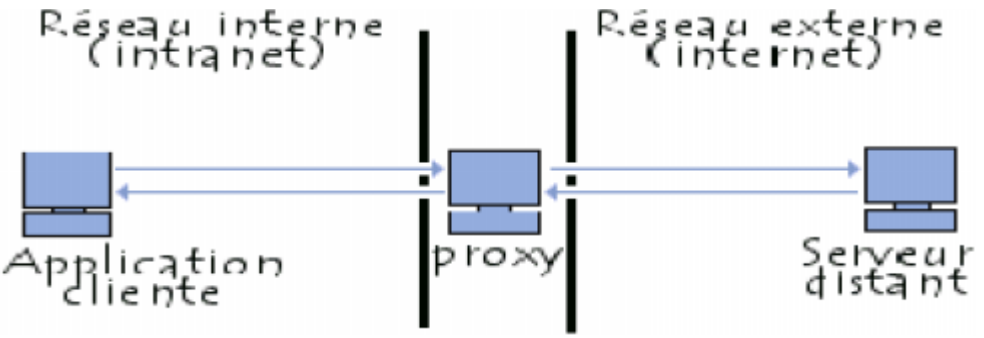


Figure II. 5: Fonctionnement d'un proxy

❖ **Les fonctionnalités d'un serveur proxy :**

- **La fonction cache :**

La plus part des proxys assurent une fonction cache c'est à-dire la capacité à garder en mémoire les pages les plus souvent visitées par les utilisateurs du réseau local afin de pouvoir les leur fournir le plus rapidement possible.

Cette fonctionnalité implémentée dans certains serveurs proxy permet d'une part de réduire l'utilisation de la bande passante vers internet ainsi que de réduire le temps d'accès aux documents pour les utilisateurs.

- **Filtrage :**

Grâce à l'utilisation d'un proxy, il est possible d'assurer un suivi des connexions (en anglais logging ou tracking) via la constitution de journaux d'activité. Il est ainsi possible de filtrer les connexions à internet en analysant d'une part les requêtes des clients, d'autre part les réponses des serveurs. Lorsque le filtrage est réalisé en comparant la requête du client à une liste de requêtes autorisées, on parle de liste blanche, lorsqu'il s'agit d'une liste de sites interdits on parle de liste noire.

- **L'authentification :**

Dans la mesure où le proxy est l'intermédiaire indispensable des utilisateurs du réseau interne pour accéder à des ressources externes, il est parfois possible de l'utiliser pour authentifier les utilisateurs, c'est-à-dire de leur demander de s'identifier à l'aide d'un nom d'utilisateur et d'un mot de passe par exemple.

II.6 Les protocoles de sécurité :

II.6.1 Protocole SSL:

Le protocole SSL (secure socket layer), le standard SSL a été mis au point par Netscape, en collaboration avec Mastercard, Bank of American. Il repose sur un procédé de cryptographie par clé publique afin de garantir la sécurité de la transmission des données sur Internet. Son principe consiste à établir un canal de communication sécurisé (chiffré) entre deux machines (un client et un serveur) après une étape d'authentification.

❖ Le principe d'une authentification du serveur avec SSL est le suivant :

1. Le navigateur du client fait une demande de transaction sécurisée au serveur.
2. Suite à la requête du client, le serveur envoie son certificat au client.
3. Le serveur fournit la liste des algorithmes cryptographiques qui peuvent être utilisés pour la négociation entre le client et le serveur.
4. Le client choisit l'algorithme.
5. Le serveur envoie son certificat avec les clés cryptographiques correspondantes au client.
6. Le navigateur vérifie que le certificat délivré est valide.
7. Si la vérification est correcte alors le navigateur du client envoie au serveur une clé secrète chiffrée à l'aide de la clé publique du serveur qui sera donc le seul capable de déchiffrer puis d'utiliser cette clé secrète. Cette clé est un secret uniquement partagé entre le client et le serveur afin d'échanger des données en toute sécurité.

Afin d'éviter des attaques, il est recommandé d'utiliser la double authentification c'est-à-dire non seulement l'authentification du serveur mais également celle du client, bien que l'authentification du client avec SSL soit facultative.

II.6.2 Protocole SSH :

Le protocole **SSH** (Secure Shell) est un protocole permettant à un client d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisée : Les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité (personne d'autre que le serveur ou le client ne

peut lire les informations transitant sur le réseau). Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames.

Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des parties croit être. Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur (spoofing).

II.6.3 S-HTTP (Secure HTTP):

S-HTTP est un procédé de sécurisation des transactions HTTP reposant sur une amélioration du protocole HTTP. Il permet de fournir une sécurisation des échanges lors de transactions de commerce électronique en cryptant les messages afin de garantir aux clients la confidentialité de leur numéro de carte bancaire ou de toute autre information personnelle.

II.6.4 IP sec (Internet Protocol Secure) :

IPsec vise à sécuriser les échanges au niveau de la couche réseau. Le réseau IPv4 étant largement déployé et la migration complète vers IPv6 nécessitant encore beaucoup de temps, il est vite apparu intéressant de définir des mécanismes de sécurité qui soient communs à la fois à IPv4 et IPv6. Ces mécanismes sont couramment désignés par le terme IPSec. Le protocole IPSec fournit ainsi :

- des mécanismes de confidentialité et de protection contre l'analyse du trafic.
- des mécanismes d'authentification des données (et de leur origine).
- des mécanismes garantissant l'intégrité des données (en mode non connecté).
- des mécanismes de protection contre le rejeu.
- des mécanismes de contrôle d'accès.

II.6.4.1les deux manières d'employer IPsec :

a. Mode transport :

Le mode transport prend un flux de niveau transport (couche de niveau 4 du modèle OSI) et réalise les mécanismes de signature et de chiffrement puis transmet les données à la couche IP. Dans ce mode, l'insertion de la couche IPsec est transparente entre TCP et IP. TCP envoie ses données vers IPsec comme il les enverrait vers IPv4.

b. Mode tunnel :

Dans le mode tunnel, les données envoyées par l'application traversent la pile du protocole jusqu'à la couche IP, puis sont envoyées vers le module IPsec. L'encapsulation IPsec en mode tunnel permet le masquage d'adresses.

Le mode tunnel est généralement utilisé entre deux passerelles de sécurité (routeur, firewall). alors que le mode transport se situe entre deux hôtes.

II.6.4.2 Les protocoles d'authentification IPsec :

❖ **a. Le protocole AH (Authentication Header protocol) :**

Le protocole AH est conçu pour assurer l'intégrité en mode non connecté et l'authentification de l'origine des datagrammes IP sans chiffrement des données (pas de confidentialité).Son principe est d'adjoindre au datagramme IP classique un champ supplémentaire permettant à la réception de vérifier l'authenticité des données incluses dans le datagramme. Ce bloc de données est appelé « valeur de vérification d'intégrité ».

❖ **b. Le protocole ESP (Encapsulating Payload Protocol):**

Le protocole ESP peut assurer, au choix, un ou plusieurs des services suivants :

- confidentialité des données et protection partielle contre l'analyse du trafic si l'on utilise le mode tunnel ;
- intégrité des données en mode non connecté et authentification de l'origine des données, protection partielle contre le rejeu.

II.7 Conclusion :

Comme c'est indiqué précédemment il existe plusieurs méthodes et mécanismes de sécurité. Néanmoins, on peut pas garantir la sécurité a un grand pourcentage (a 100%) mais ils suffit juste de bien savoir le bon fonctionnement des éléments qui interviennent dans la conception du réseau (routeur ,Switch ,firewall ,….) pour les configurer selon une politique de sécurité qui doit être définie avant la mise en œuvre du réseau .

III.1 Introduction :

Les entreprises qui cherchent à déployer des technologies de sécurité réseau pour protéger leurs intranets contre des hôtes inconnus doivent faire leur choix en fonction du niveau de sécurité souhaité, du prix et de la facilité de déploiement. Et pour cela une norme **IEEE 802.1x** a été mise en œuvre dont l'objectif principale est d'autoriser l'accès physique aux utilisateurs souhaitant à se connecter au réseau local via un Switch après une phase d'authentification.

III.2 Définition de l'authentification/ identification :

Avant toute chose, il est important de savoir de quoi on parle lorsqu'on traite l'authentification dans le domaine de l'informatique. L'authentification est la procédure qui consiste, pour un système informatique, à vérifier l'identité d'une entité (personne, ordinateur...), afin d'autoriser l'accès de cette entité à des ressources (systèmes, réseaux, applications...). L'authentification permet donc de valider l'authenticité de l'entité en question.

Dans le cas d'un individu, l'authentification consiste, en général, à vérifier que celui-ci possède une preuve de son identité ou de son statut, sous l'une des formes (éventuellement combinées) suivantes :

- Ce qu'il sait (nom d'utilisateur/mot de passe).
- Ce qu'il possède (carte à puce, certificat électronique, clé-USB, etc.).
- Ce qu'il est (caractéristique physique, biométrie).

III.3 L'authentification pour quoi faire :

L'objectif principal de l'authentification est de :

- **Sécuriser un réseau filaire ou sans-fil.**
- **Contrôle permanent de l'intégrité et de l'accès physique à un contenu ou à un service.**
- **interdire les inconnus.**
- **placer les postes connus à des endroits spécifiques du réseau (vlan) de façon dynamique.**
- **savoir quelle machine est connectée et ou est connectée.**

III.4 Les protocoles de transport sécurisés :

Un protocole de transport sécurisé permet de porter l'information d'un lieu à un autre suivant des règles prédéfinis sans que l'objet transporté ne soit en danger.

Étant donné que la majorité des réseaux utilisés à travers le monde sont de type TCP/IP

et que le choix des entreprises se porte souvent vers ce type de réseaux, nous présentons les solutions sécurisées proposées pour ces types de réseaux.

III.4.1 Le protocole ppp :

Le 802.1x est une pyramide de protocoles dont la base est l'EAP. Pour comprendre le 802.1x, il faut donc comprendre l'EAP. Et pour bien comprendre l'EAP, il faut revenir à son origine : si vous avez déjà lancé une connexion à Internet via un modem téléphonique classique votre ordinateur a commencé par établir une connexion avec une sorte de central téléphonique composé d'une batterie de modems eux-mêmes reliés à Internet. Ce central, mis en œuvre par un Fournisseur d'Accès à Internet (FAI) s'appelle un point de présence (Point of Presence, PoP). La connexion entre votre modem et l'un des modems du PoP repose sur un protocole très répandu : le Protocole de Point à Point (Point-to- Point Protocol, PPP), décrit dans la RFC 1661 et quelques RFC associées.

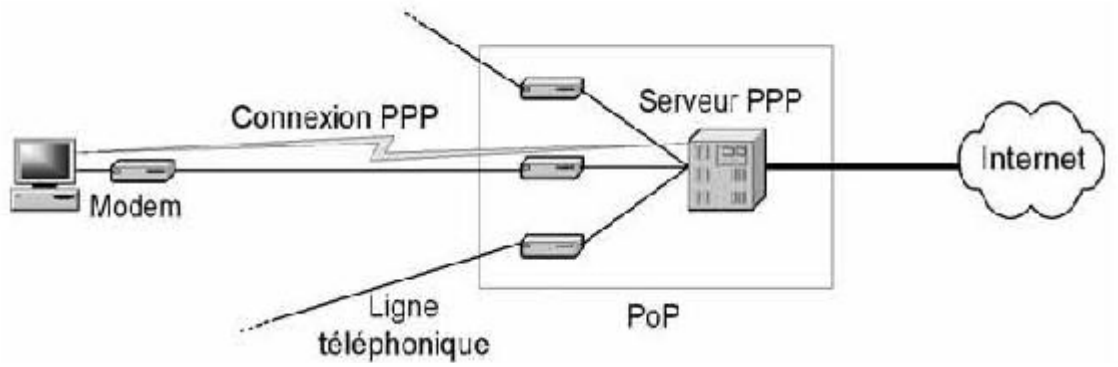


Figure III.1 : Une connexion RTC avec le protocole PPP.

Le PPP définit notamment comment vous devez vous identifier : un mot de passe vous a été attribué par votre FAI, et vous devez simplement prouver que vous le connaissez. Si c'est le cas, le PoP vous laisse passer vers Internet, sinon, vous recevez un refus catégorique et la connexion est interrompue.

III.4.1.1 PAP :

Le Protocol PAP (Password Authentication Protocol), utilisé avec le protocole PPP, permet d'identifier un utilisateur auprès d'un serveur PPP en vue d'une ouverture de connexion sur le réseau. Après une phase de synchronisation entre le client et le serveur pour définir l'utilisation du protocole PPP et PAP, le processus d'authentification se fait en deux étapes :

- Le client envoie son nom PAP ainsi que son mot de passe en clair.
- Le serveur qui détient une table de noms d'utilisateurs et de mots de passe

vérifie que le mot de passe correspond bien à l'utilisateur et valide ou rejette la connexion.

PAP est le plus simple des protocoles d'authentification, il est donc très facile à implémenter. Mais étant donné que le mot de passe circule en clair sur le réseau, c'est aussi le moins sécurisé et il est donc fortement déconseillé car il ne procure aucune sécurité. D'autre part, même si le mot de passe est crypté, il est toujours possible d'utiliser un sniffer afin de capturer la requête d'authentification.

III.4.1.2 CHAP :

Le protocole (CHAP Challenge Handshake Authentication Protocol) est défini dans la RFC 1994. Le serveur commence par envoyer un « défi » au client (16 octets aléatoires), ainsi qu'un compteur qu'il incrémente à chaque fois qu'il lance un défi. Le client doit alors passer le compteur, son mot de passe et le défi au travers d'un algorithme de hachage, habituellement l'algorithme MD5. Le résultat est une séquence de bits pseudo-aléatoires qu'on appelle le « hash » (de 16 octets dans le cas de MD5). Ce hash est envoyé au serveur, qui peut alors effectuer le même calcul et vérifier si son résultat concorde avec celui du client. Cet algorithme permet d'éviter que le mot de passe soit transféré, et évite également qu'unpirate ne répète simplement une authentification réussie qu'il aurait enregistrée auparavant, puisque le défi change à chaque authentification. Il ne permet cependant pas au client de s'assurer de l'identité du serveur.

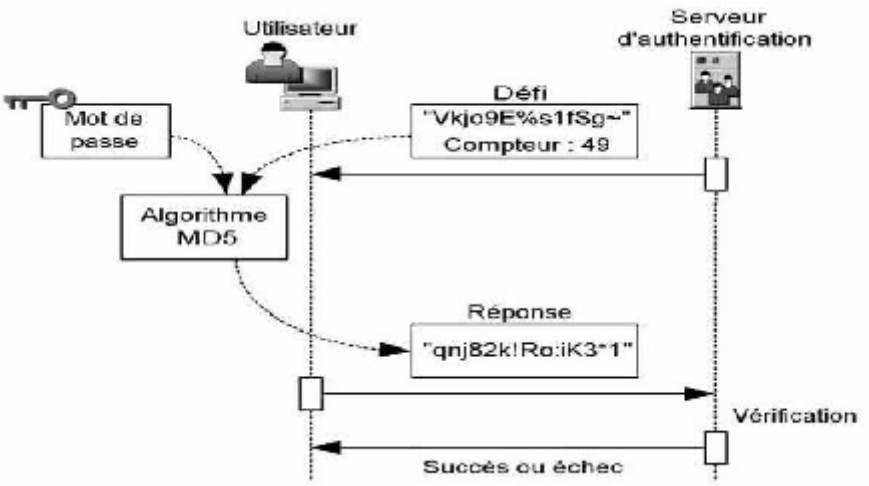


Figure III.2: L'identification avec le protocole CHAP.

III.4.1.3 MS-CHAP :

Ce protocole, souvent appelé MS-CHAP-v1, a été défini par Microsoft dans la RFC 2433. Il s'agit d'une variante de CHAP, destinée à en améliorer la sécurité. L'un des problèmes de CHAP est le fait qu'il soit nécessaire de stocker le mot de passe en clair sur le serveur : sinon, impossible de calculer le hash et de vérifier l'identité du client. Toute personne ayant accès à la base de données des utilisateurs peut donc voir les mots de passe de tout le monde. Pour éviter cela, MSCHAP spécifie que le serveur doit stocker non pas le mot de passe, mais le résultat d'un hash sur ce mot de passe (selon un algorithme propriétaire de Microsoft).

Lorsque l'utilisateur saisit son mot de passe, celui-ci doit d'abord être passé au travers du même algorithme de hash avant de suivre la procédure habituelle de CHAP. Malheureusement, MS-CHAP comporte des failles de sécurité (dues en particulier au hash propriétaire de Microsoft) qui l'ont rendu rapidement obsolète : seuls quelques vieux systèmes Windows 95/98 l'utilisent encore.

III.4.1.4 MS-CHAP-v2 :

Suite à la découverte des failles de sécurité dans MS-CHAP, Microsoft a réagi en concevant cette version 2, définie dans la RFC 2759. Nettement plus robuste, ce protocole fournit notamment un mécanisme d'authentification mutuelle : le serveur s'assure de l'identité du client, et vice versa, ce qui n'est pas le cas avec les méthodes d'authentification précédentes. Le MS-CHAP-v2 est largement utilisé dans les réseaux, Windows depuis la version Windows 2000.

III.5 Authentification par adresse MAC :

Pour de nombreux réseaux d'entreprise, le risque le plus important lié au déploiement de 802.1X et/ou NAC (Network Access Control) est la notion de « tout ou rien» qui rend un potentiel retour en arrière délicat si quelque chose venait à ne pas se dérouler correctement. Pour réduire ce risque, de nombreux administrateurs réseau et responsables sécurité, ont commencé à déployer « l'authentification par adresse MAC » comme première étape afin de sécuriser un peu plus la couche d'accès réseau. L'authentification MAC est particulièrement utile car elle adresse plusieurs objectifs menant à l'exploration de NAC et 802.1X, comme sécuriser la périphérie du réseau d'entreprise, identifier tous les équipements attachés au réseau, fournir un accès réseau aux invités, maintenir un historique de la localisation et de l'adressage de chaque

équipement, et autres. De plus, le déploiement de l'authentification par adresse MAC s'appuie sur les systèmes et les protocoles directement impliqués dans le déploiement de 802.1X. Indépendamment de la durée d'implémentation ou du nombre de phases définies, l'authentification par adresse MAC se justifie pleinement comme première phase d'un déploiement ayant pour objectif 802.1X et/ou NAC.

III.6 AUTHENTIFICATION 802.1X:

Le protocole 802.1X définit un contrôle d'accès réseau par port ainsi qu'une méthode d'authentification qui permet de restreindre l'accès aux clients non authentifiés qui se connecteraient à des ports « libres » du réseau local. On définit comme « port » le moyen par lequel un équipement client accède à des ressources partagées via un réseau (MAN ou LAN). Un port peut tout aussi bien être physique (port d'un équipement de commutation) ou virtuel (port sur une borne d'accès WIFI).

- **Le 802.1X se base sur trois éléments :**

« **Supplicant** » : le client demandant à s'authentifier avant de pouvoir accéder aux ressources du réseau.

« **Authenticator** » : l'authentificateur est l'équipement réseau (commutateur, point d'accès…) auquel le client se connecte. Suivant la réponse du serveur d'authentification, le commutateur laissera passer ou non le trafic du client.

« **Authentication server**» : le serveur d'authentification vérifie sur demande du commutateur si le demandeur peut ou non accéder aux ressources réseau LAN.

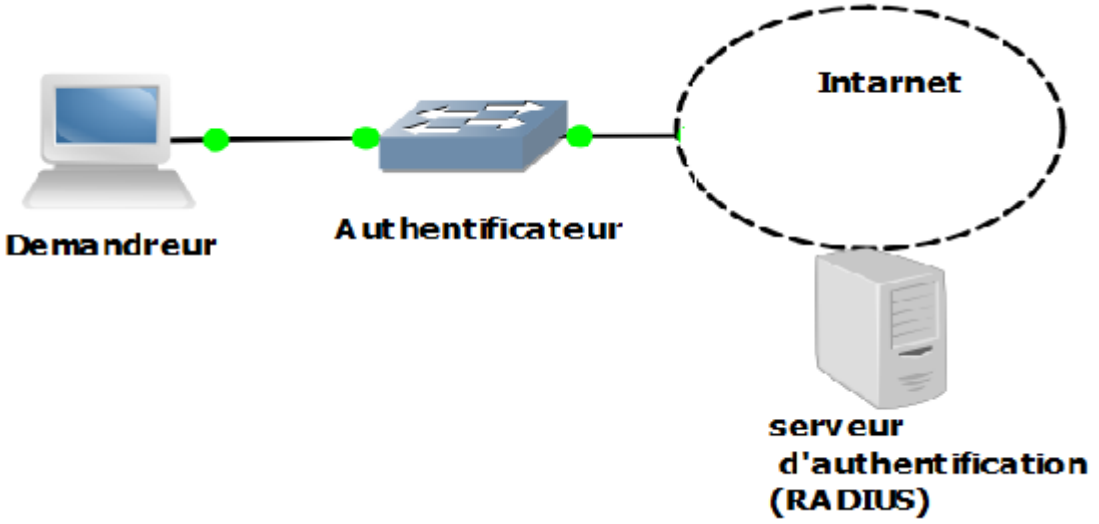


Figure III.3 Les éléments de l'authentification IEEE 802.1X pour des réseaux filaires.

III.6.1 Les méthodes d'authentification de 802.1x

III.6.1.1Le protocole EAP :

III.6.1.1.a Définition :

La communication entre l'équipement réseau (authenticator) et le serveur d'authentification est assurée par le protocole EAP (Extensible Authentication Protocol), le 802.1X ne fournissant qu'un cadre fonctionnel à l'interaction entre les équipements. Ce protocole EAP est un protocole de transport des informations d'authentification et permet d'utiliser différentes méthodes d'authentification d'où le terme '' Extensible''. Le domaine d'application de ce protocole correspond donc à tous les modes de connexion pouvant être considérés comme des connexions dites point à point telles que : connexion réseau sans fil entre un poste utilisateur et une borne d'accès, connexion filaire entre un poste utilisateur et un commutateur.

On distingue deux types de trafic EAP :

- EAP over LAN (EAPOL) : entre le système à authentifier et le point d'accès.
- EAP over Radius : entre le point d'accès et le serveur d'authentification.

III.6.1.1.b Les méthodes associées à EAP :

Le protocole EAP ne propose pas une seule méthode d'authentification mais plusieurs types d'authentification. Ainsi, une méthode d'authentification EAP utilise différents éléments pour identifier un client :

- Login / mot de passe
- Certificat électronique
- Biométrie
- Puce (SIM)

Certaines méthodes combinent plusieurs critères (certificat et login/mot de passe …). En plus de l'authentification, EAP gère la distribution dynamique des clés de chiffrement, parmi les méthodes de l'authentification les plus communes sur EAP on distingue :

a. EAP- TLS: (EAP Transport Layer Security) :

A été crée par Microsoft et accepté par l'IETF comme RFC 2716. En effet il utilise deux certificats numériques, le serveur et le client s'authentifier mutuellement tout en cryptant

les données échangées dans cette phase d'authentification. L'utilisation de clés publiques et privées des deux cotés permettre de créer un tunnel sécurisé entre les deux parties, ce qui garantit l'intégrité des données. Avec ce principe le client ne fournit pas de mot de passe, le certificat permettant l'authentification.

L'utilisation de certificat possède des avantages et des inconvénients. Ils sont souvent considérés comme plus sûrs que les mots de passe, cependant les opérations de gestion qu'ils engendrent peuvent se révéler fastidieuses (création, suppression, listes de révocation etc.) et l'existence d'une infrastructure de gestion de clés (IGC) est requise. La distribution des certificats aux clients est une contrainte qu'il ne faut pas négliger.

EAP-TLS : est implémenté chez de nombreux fabricants de matériel sans fil**.**

b. EAP-TTLS: (EAP Tunneled Transport Layer Security) et EAP-PEAP (Protected EAP):

Ces deux méthodes sont assez similaires**,** propriétaires développés par Microsoft, Cisco, RSA Security. Elles s'appuient sur la confidentialité proposée par l'encapsulation dans un tunnel pour réaliser une authentification via login/mot de passe.

On distingue deux phases d'authentification :

- Première phase : identification du serveur par le client en utilisant un certificat (validé par une autorité de certification)
- Deuxième phase : identification du client par le serveur par login/password.

À l'issue de la première phase, le tunnel TLS chiffré s'établit, garantissant une grande confidentialité des échanges pour la phase 2 où le client transmet ses éléments d'authentification (login/password) via CHAP, PAP, MS-CHAP ou MS-CHAPv2 pour EAP-TTLS et MS-CHAPv2, token-card ou certificat (similaire à EAP-TLS) pour EAP-PEAP.

La différence principale entre EAP-PEAP et EAP-TTLS vient de la manière d'encapsuler les échanges lors de la deuxième phase. Pour EAP-PEAP, les données échangées entre le client et le serveur au travers du tunnel TLS sont encapsulées dans des paquets EAP. EAP-TTLS utilisent des AVP (Attribute-Values Pairs) encapsulées dans des paquets EAP-TTLS.

L'avantage présenté par ces deux méthodes vient du fait que le client peut être authentifié par mot de passe, on supprime donc la complexité de gestion liée aux certificats caractéristique d'EAP-TLS, tout en proposant une authentification mutuelle.

PEAP est proposé nativement dans Windows XP et Windows 2000, ce qui peut grandement faciliter son déploiement.

c. EAP-MD5 (EAP Message Digest 5-Challenge):

Cette méthode ne propose pas une authentification mutuelle, le client s'authentifie simplement en fournissant un couple login/mot de passe. Grace au mécanisme de challenge/ réponse, le serveur envoie un challenge au client, celui-ci renvoie son mot passe associé au challenge, le serveur compare le résultat avec le mot de passe qu'il détient dans sa base plus le challenge envoyé, si le résultat est identique alors l'accès est autorisé, sinon il est refusé.

Le problème majeur de cette méthode réside le fait que les échanges ne sont pas chiffrés, en outre EAP-MD5 ne gère pas la distribution dynamique des clés WEP.

Le seul avantage de cette méthode est la simplicité : il est relativement facile de mettre en place une structure d'authentification basée sur cette méthode, celle-ci est d'ailleurs beaucoup utilisée pour des réseaux filaires ou la contrainte lié au chiffrage des échanges est moins forte que pour les réseaux wifi.

d. LEAP (Light weight EAP):

Est une implémentation propriétaire d'EAP conçu par Cisco système, assurant une authentification simple par mot de passe via une encapsulation sécurisée.

Ce protocole est vulnérable aux attaques (cryptage MD5) sauf si l'utilisateur utilise des mots de passe complexes.

III.7 La norme 802.1x :

III.7.1 Définition :

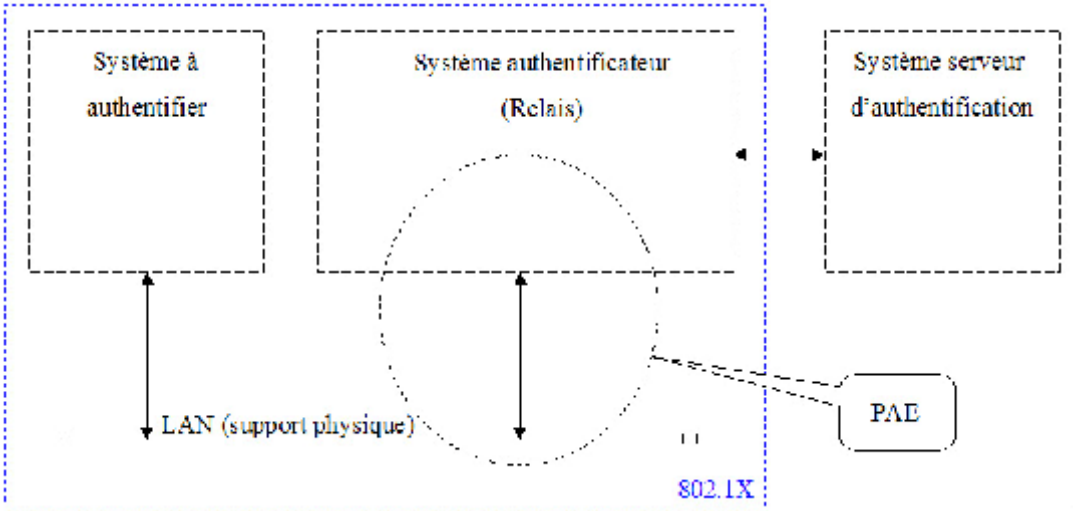
Ce standard mis au point par l'IEEE en juin 2001, a comme objectif de réaliser une authentification de l'accès au réseau au moment de la connexion physique à ce dernier. Cette authentification intervient avant tout mécanisme d'autoconfiguration (ex. DHCP).Dans la plupart des cas, le service autorisé en cas de succès est le service Ethernet. L'objectif de ce standard est donc uniquement de valider un droit d'accès physique au réseau, indépendamment du support de transmission utilisé, et en s'appuyant sur des mécanismes d'authentification existants.

III.7.2 Le modèle et les concepts du standard IEEE :

Dans le fonctionnement du protocole, les trois entités qui interagissent sont le système à authentifier (supplicant), le système authentificateur (authenticator system) et un

serveur d'authentification (authentication server). Le système authentificateur contrôle une ressource disponible via le point d'accès physique au réseau, nommé PAE (Port Access Entity). Le système à authentifier souhaite accéder à cette ressource, il doit donc pour cela s'authentifier.

Dans cette phase d'authentification 802.1X, le système authentificateur se comporte comme un mandataire (proxy) entre le système à authentifier et le serveur d'authentification ; si l'authentification réussit, le système authentificateur donne l'accès à la ressource qu'il contrôle. Le serveur d'authentification va gérer l'authentification proprement dite, en dialoguant avec le système à authentifier en fonction du protocole d'authentification utilisé.



Figue III.4 Les entités qui interagissent dans 802.1x

C'est au niveau du PAE que porte l'essentiel des modifications introduites par le protocole 802.1x. Dans la plupart des implémentations actuelles, le système authentificateur est un équipement réseau (par exemple un commutateur Ethernet, une borne d'accès sans fil, ou un commutateur/routeur IP), le service dont il contrôle l'accès est le service Ethernet (ou le routage des datagrammes IP). Le système à authentifier est un poste de travail ou un serveur. Le serveur d'authentification est typiquement un serveur Radius, ou tout autre équipement capable de faire de l'authentification.

III.7.3 Le point d'accès au réseau (PAE) :

La principale innovation amenée par le standard 802.1X consiste à scinder le port d'accès physique au réseau en deux ports logiques, qui sont connectés en parallèle sur le port physique. Le premier port logique est dit « contrôlé », et peut prendre deux états

« Ouvert » ou « fermé ». Le deuxième port logique est, lui, toujours accessible mais il ne gère que les trames spécifiques à 802.1X.

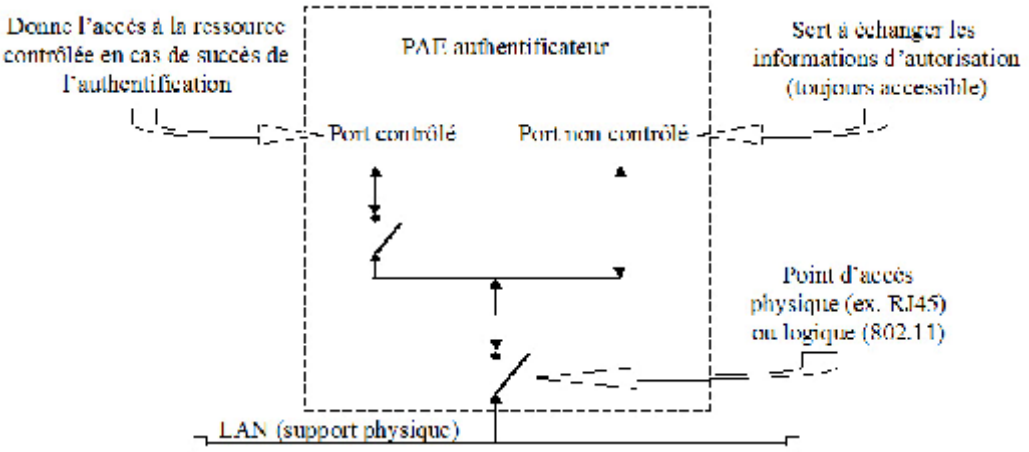


Figure III.5 Le PAE

- **Ports contrôlés et non contrôlés de PAE :**

IEEE 802.1X définit les types de ports logiques suivants qui accèdent à un intranet via un port LAN physique unique :

- **Port non contrôlé** :

Il permet à l'authentificateur direct de communiquer avec d'autres nœuds sur l'intranet (tels que le serveur d'authentification). Les trames envoyées par les demandeurs ne sont jamais envoyées à l'aide du port non contrôlé.

- **Port contrôlé** :

Il permet à un demandeur d'échanger des trames avec les nœuds sur l'intranet, uniquement si le demandeur est authentifié et autorisé par 802.1X. Avant l'authentification et l'autorisation, le port contrôlé est bloqué et aucune trame ne circule entre le demandeur et l'intranet. Lorsque le demandeur est authentifié et autorisé, le port s'ouvre et les trames peuvent circuler entre le demandeur et les nœuds sur l'intranet.

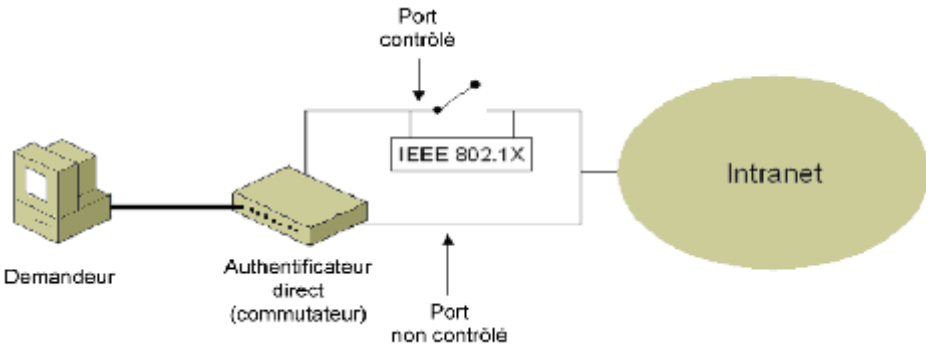


Figure III.5 les ports de PAE

III.7.4 Fonctionnement général du protocole :

III.7.4.1 La circulation des paquets d'authentification :

Le standard 802.1X ne crée pas un nouveau protocole d'authentification, mais s'appuie sur les standards existants. Le dialogue entre le système authentificateur et le système à authentifier se fait en utilisant le protocole EAP. Les paquets EAP sont transportés dans des trames Ethernet spécifiques EAPOL (EAP Over Lan), ce qui permet une encapsulation directe d'EAP dans Ethernet. Le dialogue entre le système authentificateur et serveur d'authentification se fait par une simple « ré-encapsulation » des paquets EAP dans un format qui convient au serveur d'authentification, sans modification du contenu du paquet par le système authentificateur.

Ce dernier effectue cependant une lecture des informations contenues dans les paquets EAPOL afin d'effectuer les actions nécessaires sur le port contrôlé (blocage ou déblocage). Ainsi, le système authentificateur débloquera le port contrôlé en cas d'authentification réussie, ou il le bloquera s'il y a une demande explicite en ce sens du système à authentifier.

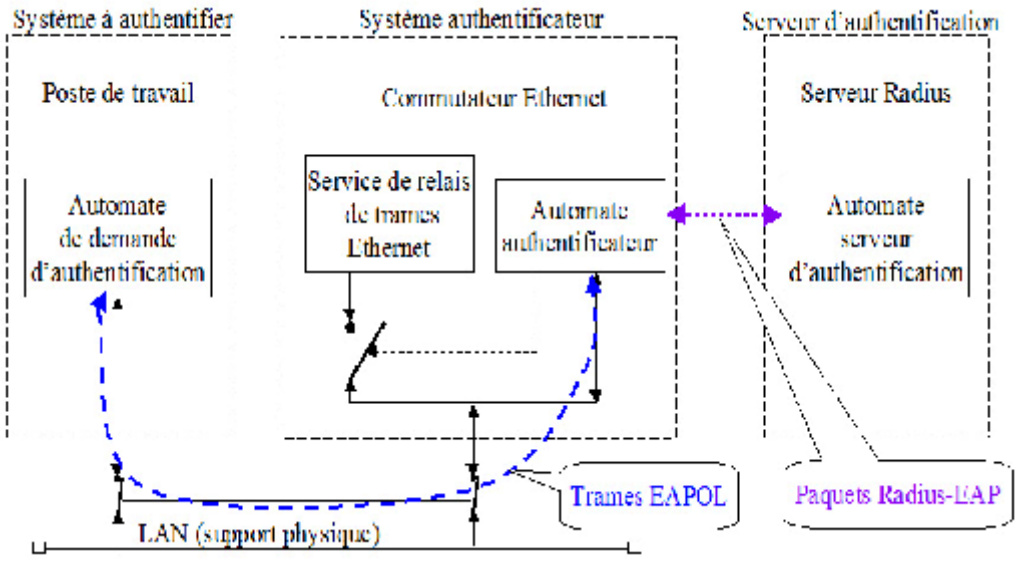


Figure III.6 : 802.1x et serveur d'authentification

III.7.4.2 Les paquets EAP et EAPOL :

On définit les quatre types de paquets EAP (champ code, sur un octet) :

Request : le système authentification émet une requête d'information.

Response : réponse du système à authentifier à un paquet request.

Success : le système authentification indique une authentification réussie.

Failure : le système authentification indique un échec de l'authentification.

Le paquet EAP contient aussi un champ identifier (sur un octet) pour identifier une session d'authentification. Dans le cas de paquets de type request ou response, un champ (type) définit la nature des informations qui sont contenues dans le paquet. Par exemple :

Identity : chaine de caractères identifiant l'utilisateur (par exemple une adresse mail, un nom de login, ect).

Notification : chaine de caractère envoyée à l'utilisateur final.

Nak : refus d'un type d'authentification et proposition d'n autre.

MD5- Challenge : défi (challenge) ou réponse (idem authentification chap).

One-Time-Password : défi ou réponse

Generic Token Ring Card : défi ou réponse.

Les trames EAPPOL peuvent être des quatre types suivants :

EAP-Packet : paquet de dialogue EAP.

EAP-Start : authentification explicitement demandée par le système s'authentifie.

EAP-Logoff : fermeture du port contrôlé explicitement demandée par le système qui s'authentifie.

EAPOL-Key : si chiffrement disponible.

EAPOL-Encapsulated-ASF-Alert.

- **Exemple de session 802.1X/EAP :**

Avant la connexion du système à authentifier au port physique du PAE du système authentificateur, le port contrôlé de ce dernier est bloqué, et seul le port non contrôlé est accessible. Lorsque le système à authentifier se connecte au port physique du système authentificateur, il reçoit un paquet EAP l'invitant à s'authentifier. Sa réponse est reçue sur le port non contrôlé du système authentificateur, puis est retransmise au serveur d'authentification par ce dernier. Par la suite, un dialogue s'établit entre le serveur d'authentification et le système à authentifier par le biais du relais offert par le port non contrôlé du PAE du système authentificateur.

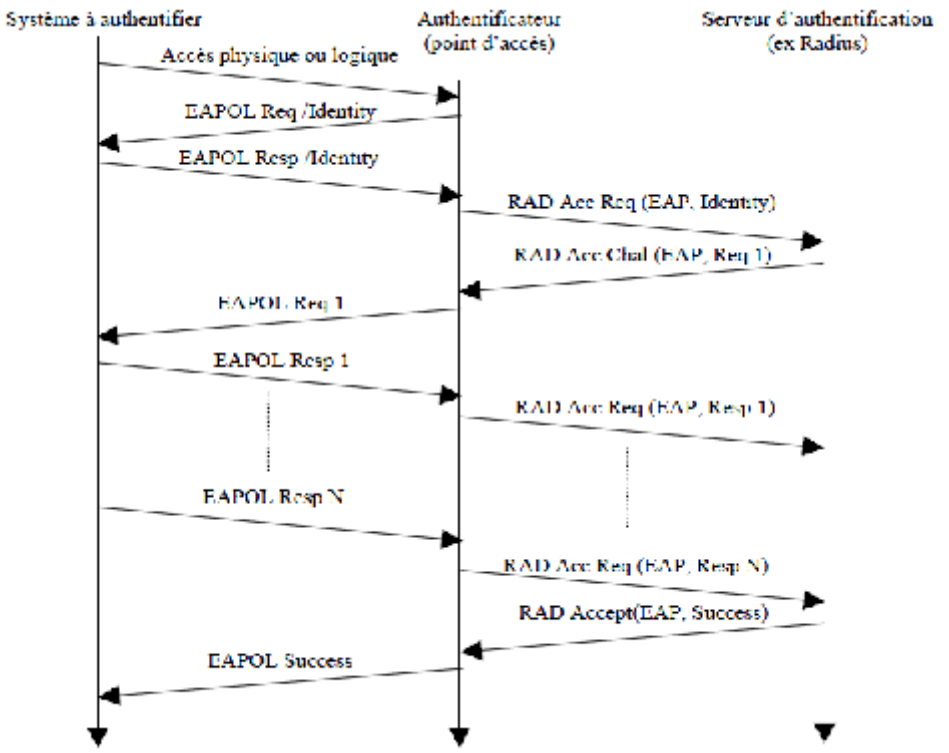


Figure III.6 : Séquence d'authentification

Quand l'automate 802.1X du système authentificateur voit passer un acquittement positif d'authentification (en provenance du serveur), il débloque son port contrôlé (interrupteur fermé), donnant ainsi au client authentifié l'accès au service

À partir de cet instant, le schéma logique du PAE du système authentificateur devient tel que décrit ci-dessous et le trafic Ethernet est assuré normalement. Cependant, les automates implémentant le protocole 802.1X restent actifs et peuvent à nouveau réactiver un processus d'authentification en cas, par exemple, de demande explicite du client ou de déconnexion physique au réseau.

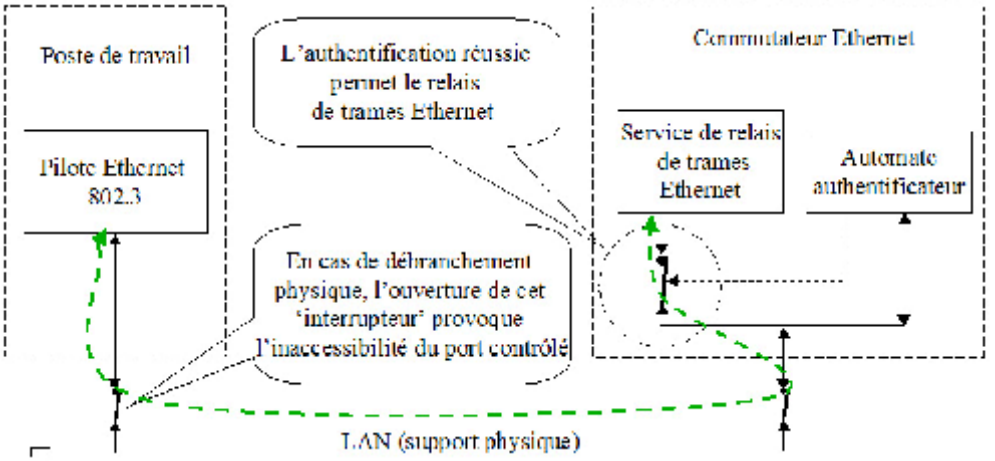


Figure III.7 Exemple de situation après une authentification réussie

III.7.5 PAE du système à authentifier :

III.7.5 .1Schéma simplifié de l'automate à états finis :

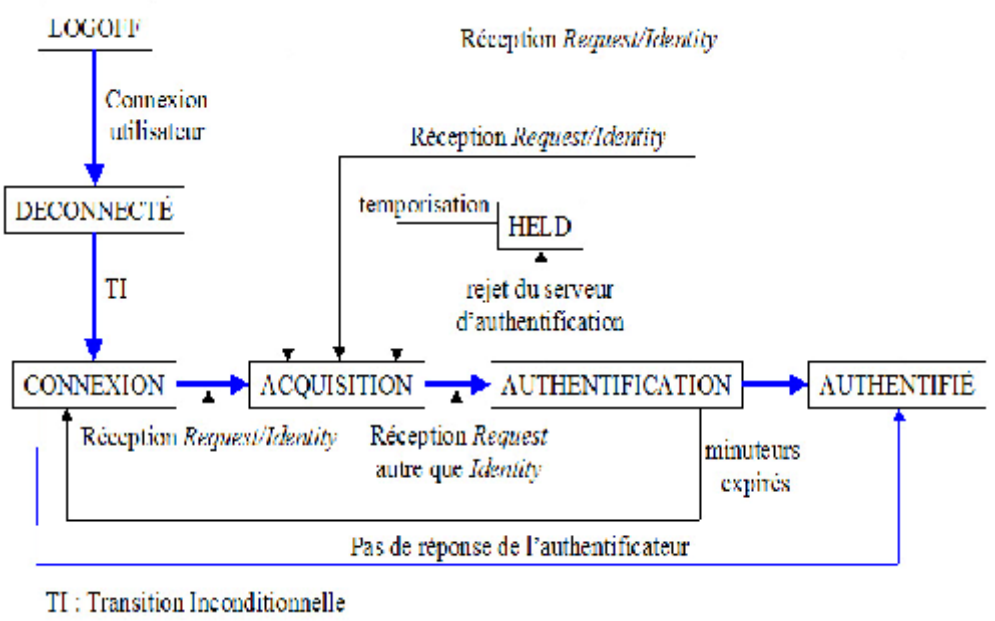


Figure III.8 Automate à état finis du système à authentifier.

III.7.5 .2 Définition des états de l'automate à états finis :

LOGOFF : cet état est atteint quand l'utilisateur du système quitte sa session. On remarquera que les concepteurs du standard permettent, par cette fonctionnalité, de relier l'état du port contrôlé à l'état de la session d'un utilisateur (à condition bien sûr que la connexion physique soit toujours active).

DÉCONNECTÉ : dans cet état, le port physique est actif (par exemple, l'équipement à authentifier est branché).

CONNEXION : l'automate du système à authentifier est en attente d'une requête EAP avec un type Identify du système authentificateur du port où il est physiquement connecté. Dès l'arrivée d'une telle requête, il passe dans l'état « ACQUISITION ». Pour permettre la compatibilité avec des équipements ne supportant pas le protocole 802.1X, le système à authentifier émet régulièrement des requêtes EAP avec un type Start. Au bout de 3 (valeur par défaut) non réponses, il passe dans l'état « AUTHENTIFIÉ » (considérant qu'il n'y a pas de PAE authentificateur sur ce port).

ACQUISITION : l'automate du système à authentifier envoie son identité au système authentificateur, et passe dans l'état « AUTHENTIFICATION » dès réception du premier paquet EAP avec un type différent d'Identify.

AUTHENTIFICATION : dans cet état, l'automate du système à authentifier répond aux requêtes du serveur d'authentification qui lui sont transmises par le système authentificateur.

AUTHENTFIER : les services contrôlés par le port protégé sont accessibles.

HELD : état de temporisation (60s par défaut) avant passage à l'état « CONNEXION ». Cette attente est une parade à une attaque de type « force brute ». Dans cet état la réception d'une requête EAP avec un type Identify provoque un passage à l'état « ACQUISITION ».

III.8 Les faiblesses de 802.1x :

- Le protocole 802.1X a été prévu pour établir une connexion physique. Donc l'insertion d'un hub permet de faire bénéficier d'autres utilisateurs de l'ouverture du port Ethernet d'un commutateur, tout en restant transparent pour le 802.1X
- Il est possible de configurer les équipements réseaux de façon à bloquer le port Ethernet si l'adresse MAC à changé.
- Il est également possible de faire des attaques par écoute, rejeu et vol de session. Les attaques sur 802.1X sont, de plus, facilitées dans le cas de l'Ethernet sans fil.
- Attention, pour que le 802.1x fonctionne correctement il faut bien l'implémenté sur les différentes machines.

III.9 Les évolutions de 802.1X :

La révision du standard 802.1X se fait par l'addendum 802.1aa, dont le dernier draft été publié en février 2003. Les principales modifications introduites concernent le non- rejeu des échanges, l'authentification mutuelle, et la gestion des clés.

L'authentification mutuelle est une amélioration importante, car elle permet de résoudre le cas où le client est lui même un fournisseur de service réseau, et a besoin d'être sûr qu'il s'adresse bien à un port 802.1X de confiance. Un exemple type concerne le cas du branchement d'un commutateur sur un autre commutateur.

III.10 Conclusion :

Dans ce chapitre nous avons présenté les différentes méthodes et protocoles utilisés pour parer aux risques liés au réseau local, cependant le choix d'une méthode de sécurisation dépendra des exigences, du matériel, de la distribution géographique et de la nature des communications de l'entreprise. De nos jours, la plus part des entreprises optent pour une solution centralisée en introduisant une architecture client /serveur capable de sécuriser les échanges dans le réseau grâce au protocole 802.1x et le serveur RADIUS.

IV.1 Introduction :

Le but de ce chapitre est de présenter le serveur d'authentification RADIUS, son principe de fonctionnement, ses caractéristiques et son implémentation .En suite nous allons introduire les annuaires utilisés par ce serveur.

IV.2 Définition de RADIUS (Remote Authentication Dial-in User Service) :

C'est un serveur d'authentification qui fonctionne en mode client-serveur permettant de centraliser des données d'authentification. Le protocole RADIUS est un protocole dit AAA pour Authentication (qui parle ?), Autorisation (quels sont ses droits ?) et Accounting (que fait-il ?). Ce protocole va nous permettre de répondre a une problématique de gestion des connexions d'utilisateurs à des services réseaux, notamment ce qui relève de la politique d'autorisation, des droits d'accès et de la traçabilité.

IV.2.1. Principe :

Le principe de fonctionnement du protocole réside dans l'utilisation d'un secret qui permet d'authentifier les transactions et d'effectuer le cryptage du mot de passe, ceci à travers de nombreux mécanismes, les plus courants étant PAP, CHAP, LDAP et KERBEROS. Contrairement au protocole TACACS +, il n'est possible de chiffrer que le mot de passe au sein de la trame. RADIUS est un protocole AAA, c'est un protocole d'authentification, d'accounting mais pourtant pas d'autorisation puisqu'elle est liée à l'authentification, ceci étant du à sa grande extensibilité. En effet le protocole repose sur la transmission d'attribut Clef/Valeur. Ces attributs per mettent d'échanger un nombre illimité d'informations entre le client et le serveur (password, Adresse MAC, …), et permettent donc aux principaux équipementiers de développer leurs propres attributs. La mise en place de RADIUS repose principalement sur l'utilisation d'un annuaire/base de données, d'un serveur maître et d'un serveur client. Le schéma ci-dessous montre un exemple courant de l'implémentation de RADIUS.

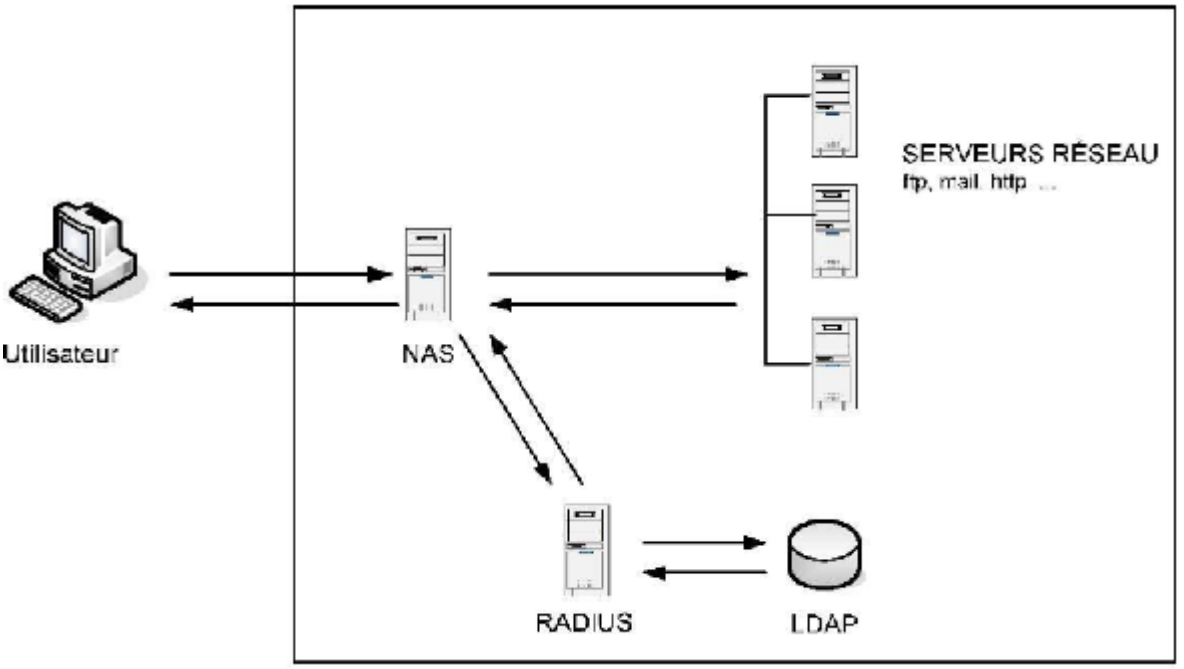


Figure IV.1: Système utilisant un serveur RADIUS

IV.3 Fonctions de RADIUS :

IV.3.1 Authentification (Identification) :

Processus permettant de garantir que la personne qui tente d'accéder au réseau dispose d'un compte valide .Le mot de passe de l'utilisateur est comparé avec les entrées figurant dans une base de données centrale.

IV.3.2 Accounting (Comptabilisation) :

La deuxième fonction d'un serveur RADIUS est l'Accounting assurant à la fois la journalisation des accès et la facturation. Gérée sur des ports UDP différents .Cette fonction est souvent assurée par un programme ou même un serveur déférent. L'accountig se base sur deux types de paquets principaux : Accounting Start et Accounting Stop, une session est définie comme l'intervalle entre un Start et un Stop .Le paquet Accounting Start émis par le client Radius après connexion effective de l'utilisateur suite à une phase d'identification réussie contient des données de base : nom d'utilisateur, adresse IP affectée, date et heur de connexion, type de connexion, type de service.

Quand l'utilisateur se déconnecte du service ou que le client Radius le déconnecte sur inactivité ,dépassement de temps de connexion ou autre ,ce client Radius envoi un paquet Accounting Stop avec le même identificateur de session ,le serveur Radius peut alors clore la

session et journaliser la déconnection ,souvent avec un grand nombre de paramètres dans le paquet Stop : temps de connexion ,type d'utilisation ,nombre de paquets et d'octets échangés selon les divers protocoles , et éventuellement des informations plus confidentielles sur les sites visités ou contenues échangés .

IV.3.3 Autorisation :

Permit à l'exploitant du réseau de définir les services réseau dont les utilisateurs finaux peuvent bénéficier. Par exemple une entreprise peut autoriser ses employés à utiliser les possibilités internet à distance à partir de leurs domiciles, mais n'autoriser qu'un accès financer par l'entreprise au réseau de cette dernière.

IV.4 Etablissement d'une session RADIUS :

Le protocole RADIUS est basé sur un échange de 4 différents types de paquets utilisant le protocole UDP.

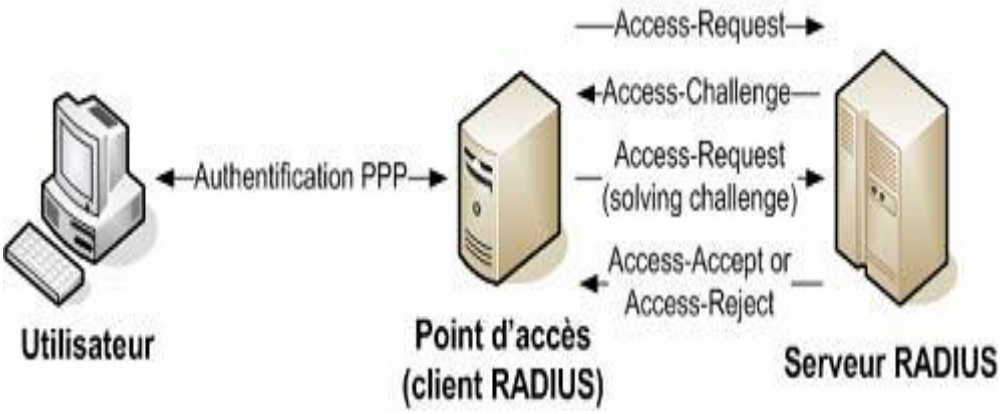


Figure IV.2 : flux de message RADIUS

- **Méthode d'authentification :**

1. Le poste utilisateur transmet les informations nécessaires à l'authentification (login, mot de passe, adresse MAC,…) au client RADIUS via une liaison PPP ou SLIP.

2. Le client RADIUS envoi un paquet « Access-Request » au serveur RADIUS. Il contient l'ensemble des informations de l'utilisateur (ID du client, mot de passe, numéro du port,…). Si un mot de passe est présent, il sera haché en utilisant le mécanisme MD5.

3. Le serveur RADIUS reçoit la requête, vérifie l'authenticité du paquet en vérifiant le secret qu'il partage avec le client RADIUS, puis vérifie l'identité de l'utilisateur en extrayant et

en comparant les informations contenues au sein d'une base de données ou d'un annuaire. Le serveur RADIUS peut demander soit de ré-emettre un access-request, soit pour demander des informations complémentaires.

4. Le client RADIUS génère ensuite une requête Access-Request contenant les informations d'authentifications demandées par le challenge.

5. Enfin, le serveur RADIUS valide ou refuse la requête en transmettant un paquet de type « Access-Accept » ou « Access-Reject ». Ce paquet peut contenir une liste de services qui sont autorisés (par exemple le vlan).

IV.5 Formats d'un paquet RADIUS :

La longueur des champs est indiquée en octets.
Le champ Attribut et valeurs est une concaténation d'attribut RADIUS et des valeurs qu'ils prennent.

Code	Identifiant	Longueur	Authentificateur	Attributs et valeurs
1	1	2	16	N

IV.5.1. Signification des différents champs :

Code : Entier indiquant le type du message transmet dans le paquet .Les paquets contenant un code invalide sont ignorés sans notification.

Identifiant : Entier permettant d'identifier la session en liant les messages entre eux .En analysant le numéro du port source, l'adresse IP, les relations temporelles entre les messages et le champ Identifier, le serveur RADIUS est capable de détecter les messages suspects et dupliqués.

Longueur : Longueur du paquet en octets.

Authentificateur (authenticator) : Ce champ est très important du point de vue de la sécurité .Il permet :

- Au client d'authentifier la réponse du serveur.
- De masquer le mot de passe en créant l'attribut User-Password.

IV.5.2 Attribut User-password :

Cet attribut contient le mot de passe de l'utilisateur à authentifier.

IV.5.3 Attribut Message-authenticator :

Cet attribut permis le contrôle d'intégrité des données échangées ainsi que l'authentification du client RADIUS et du serveur RADIUS.
Cet attribut est optionnel .Cependant, lorsque RADIUS est utilisé avec 802.1X, il est obligatoire.

IV.5.4 Secret partagé :

Afin de renforcer la sécurité, RADIUS implémente le concept de secret partagé**.** Un secret partagé est une chaine de caractères connue uniquement par le client RADIUS et le serveur RADIUS. Cette valeur est utilisée dans les mécanismes et les champs Response Authenticator, User-Password et Message authenticator.

IV.6 Limitations :

On défini certaines limites du serveur RADIUS :

- RADIUS a été conçu pour des identifications par modem, sur des liaisons lentes et peut sures ;c'est la raison du choix du protocole UDP .Ce choix technique d'un protocole conduit à des échanges laborieux basés sur des temporisations de réemission,des échanges d'accusés de réception qui se justifiaient tant que la connexion à l'internet relevait du principe d'UDP .

- RADIUS assure un transport en clair, seul le mot de passe est chiffré par hachage ; la sécurité toute relative du protocole repose sur le seul shared secret et impose la sécurisation des échanges entre le client et le serveur par sécurité physique ou VPN.

- RADIUS est strictement client-serveur, d'où des discussions de protocole propriétaires quand un serveur doit légitimement arrêter une session.

- RADIUS n'assure pas de mécanisme d'identification du serveur ; or se faire passer pour un serveur est un excellent moyen de récolter des noms et mots de passe. EAP assure une identification mutuelle du client et du serveur.

IV.7 Implémentation du serveur RADIUS :

- **IAS (Internet Authentication Service) :**

IAS est le service d'authentification internet sur Windows 2000(serveur IAS) et Windows Server 2003 (service IAS) .C'est une implémentation Microsoft du serveur RADIUS : Le service IAS joue le rôle du serveur RADIUS .Il effectue une authentification, une autorisation et une gestion des comptes centralisés des connexions pour de nombreux types d'accès réseau (accès sans fil, accès par commutateur d'authentification, accès par connexion à distance et VPN). En tant que proxy RADIUS, le service IAS peut envoyer les messages d'authentification et de gestion de comptes à d'autres serveurs RADIUS.

- **NAP (Network Access Protection) :**

NAP est une nouvelle protection de l'accès réseau dans Windows server .Il offre de nouvelles possibilités au niveau stratégies de sécurité : par exemple il peut demander que les entités du réseau possèdent les dernières mises à jour du système d'exploitation et les dernières fiches de signatures antivirus .En fonction de cela, les entités auront plus ou moins de droits sur le réseau. Ces entités sont appelés client NAP.

IV.8 Annuaires :

Un **annuaire** est une bibliothèque (imprimée ou électronique) mise à jour régulièrement qui regroupe des informations (nom, adresse, coordonnées, etc.) sur les membres d'une association, d'une entreprise ou d'un organisme professionnel, ou sur les abonnés à un service.

IV.8.1 LDAP (Lightweight Directory Access Protocol):

LDAP est normalisé par l'IETF .Il s'agit d'un protocole d'interrogation d'annuaire. On dit qu'il est allégé, par comparaison à la norme X500, son ancêtre, dont la mise en œuvre était très lourde. LDAP regroupe les données d'une entité au même endroit .On dit que c'est un annuaire fédérateur .C'est un standard incontournable : la plupart des applications récentes s'appuient dessus : les outils de messageries, les actifs du réseau (proxy, firewall…), les progiciels de gestion, les intranets etc.

Une majorité de logicielles utilisent LDAP pour l'authentification .LDAP est une base de données hiérarchique et non pas relationnelle. LDAP propose donc des mécanismes pour gérer l'authentification. Plusieurs méthodes sont possibles en fonction du niveau de sécurité désiré :

- La connexion anonyme est généralement limitée à la consultation de parties restreintes de l'annuaire.
- L'authentification par login /mot de passe.
- L'authentification par login/mot de passe avec hachage de ce dernier.
- L'authentification par login /mot de passe sur TLS avec un tunnel TLS entre le client et l'application et un tunnel TLS entre l'application et l'annuaire.
- L'authentification par certificat X509.

IV.8.2 Active Directory :

IV.8.2 .1 Présentation du service Active Directory :

Active Directory est un annuaire système hiérarchique .Il permet de localiser, rechercher et gérer des ressources représentées par des objets de l'annuaire .Il offre des mécanismes de sécurité pour protéger ses informations .Il permet de gérer des ressources liées à la gestion du réseau (domaines, comptes utilisateurs, stratégies de sécurité etc …). La base de données d'AD est distribuée ce qui lui améliore la tolérance aux pannes. Active Directory est capable d'interagir avec des clients et des serveurs LDAP d'autres origines.

Certains produits Microsoft sont installés par défaut (ou fortement conseillés lors de l'installation) : DNS, serveur Web .D'autres bénéficient d'une forte intégration avec AD (serveur de courrier Exchange, ISA Server). Active Directory centralise l'authentification .Le contrôle d'accès peut être défini à la fois sur chaque objet de l'annuaire. Il fournit non seulement le stockage mais également l'étendue d'application des stratégies de sécurité.

Quels que soit les qualités des produits concurrents (serveurs Apaches, annuaire open-ldap ou novell, serveur DNS etc.…), leurs mise en place sera forcement moins naturelle que celle des produits Microsoft, le support par AD d'un certain nombre de protocoles standard a pour but de fédérer l'ensemble des ressources réseau autours de serveurs Microsoft.

Le service Active Directory (AD) permet une gestion centralisée. Cela vous donne la possibilité d'ajouter, de retirer et de localiser les ressources facilement.
Ainsi, nous avons :

- **Une administration simplifiée :** Active Directory offre une administration de toutes les ressources du réseau d'un point unique. Un administrateur peut se connecter sur n'importe quel ordinateur pour gérer les ressources de tout ordinateur du réseau.
- **Une mise à l'échelle :** Active Directory permet de gérer des millions d'objets répartis sur plusieurs sites si cela est nécessaire.

- **Un support standard ouvert :** Active Directory utilise DNS pour nommer et localiser des ressources, ainsi les noms de domaine Windows 2003 sont aussi des noms de domaine DNS.

Active Directory fonctionne avec des services de clients différents tels que NDS de Novell. Cela signifie qu'il peut chercher les ressources au travers d'une fenêtre d'un navigateur web.

IV.8.2.2 Objets Active Directory :

Active Directory stocke des informations sur les objets du réseau. Il en existe de plusieurs types :

IV.8.2.3 Structure d'Active Directory :

La structure d'Active Directory est hiérarchique, elle se décompose comme suit :

IV.8.2.3.a Structure logique d'Active Directory :

- **Les Domaines :**

Unité de base de la structure Active Directory, un domaine est un ensemble d'ordinateurs ou d'utilisateurs qui partagent une même base de données d'annuaire. Un domaine a un nom unique sur le réseau.

Dans un environnement Windows 2000/2003, le domaine sert de limite de sécurité. Le rôle d'une limite de sécurité est de restreindre les droits d'un administrateur ou de tout autre utilisateur avec pouvoir uniquement aux ressources de ce domaine et que seuls les utilisateurs explicitement promus puissent étendre leurs droits à d'autres domaines.

Dans un domaine Windows 2000/2003, tous les serveurs maintenant le domaine (contrôleurs de domaine) possèdent une copie de l'annuaire d'Active Directory. Chaque contrôleur de domaine est capable de recevoir ou de dupliquer les modifications de l'ensemble de ses homologues du domaine.

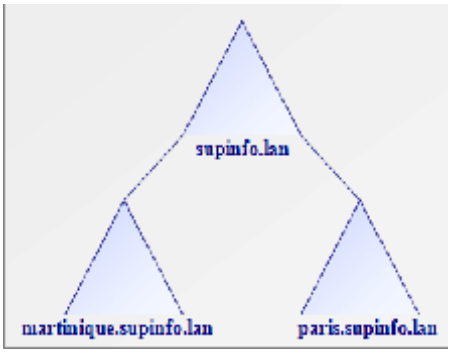
❖ **Unité organisationnelle (OU) :**

Une unité d'organisation est un objet conteneur utilisé pour organiser les objets au sein d'un domaine. Il peut contenir d'autres objets comme des comptes d'utilisateurs, des groupes, des ordinateurs, des imprimantes ainsi que d'autres unités d'organisation. Les unités d'organisation permettent d'organiser de façon logique les objets de l'annuaire (ex: représentation physique des objets ou représentation logique). Les unités d'organisation permettent aussi de faciliter la délégation de pouvoir selon l'organisation des objets.

❖ **Les Arborescences :**

Le premier domaine installé est le domaine racine de la forêt. Au fur et à mesure que des domaines lui sont ajoutés, cela forme la structure de l'arborescence ou la structure de la forêt, selon les exigences pour les noms de domaine.

Une **arborescence** est un ensemble de domaines partageant un nom commun. Par exemple, supinfo.lan est le domaine parent du domaine paris.supinfo.lan et du domaine martinique.supinfo.lan.



❖ **Forêt :**

C'est un groupement ou un arrangement hiérarchique d'un ou plusieurs arbres qui ont des noms disjoints (par exemple : laboratoire-microsoft.org et supinfo.com). Tous les arbres d'une forêt partagent le même schéma commun et le même catalogue, mais ont des structures de noms différentes. Les domaines d'une forêt fonctionnent indépendamment les uns des autres, mais les forêts permettent la communication d'un domaine à l'autre.

❖ **Objet :**

Représente une ressource du réseau qui peut-être par exemple un ordinateur ou un compte utilisateur.

❖ **Classe :**

Description structurelle d'objets tels les comptes d'utilisateurs, ordinateurs, domaines, ou unités organisationnelles.

IV.8.2.3.b Structure Physique d'Active Directory :

- **Contrôleurs de domaine :**

Un contrôleur de domaine est un ordinateur exécutant Windows 2003 Server qui stocke un répliqua de l'annuaire. Il assure la propagation des modifications faites sur l'annuaire. Il assure l'authentification et l'ouverture des sessions des utilisateurs, ainsi que les recherches dans l'annuaire. Un domaine peut posséder un ou plusieurs contrôleurs de domaine. Dans le cas d'une société constituée de plusieurs entités dispersées géographiquement, on aura besoin d'un contrôleur de domaine dans chacune de ses entités.

- **Sites :**

Un site est une combinaison d'un ou plusieurs sous réseaux connectés entre eux par une liaison à haut débit fiable (liaison LAN). Définir des sites permet à Active Directory d'optimiser la duplication et l'authentification afin d'exploiter au mieux les liaisons les plus rapides.

V.1 Introduction :

Une grande partie des attaques et des problèmes de sécurité rencontrés dans un réseau informatique ne provient pas de l'extérieur mais elle a une source intérieure au réseau. Donc il est nécessaire de contrôler l'accès physique au LAN en implémentant une méthode de sécurisation (**norme 802.1x**) qui permet l'authentification des clients qui veulent se connecter au réseau. Lorsque le client veut accéder au point d'accès (Switch) il doit utiliser **la norme 802.1x**.

V.2 Infrastructure :

Comme définit dans le chapitre trois, les trois types entités principales interviennent dans le mécanisme d'authentification **802.1x** sont :

- **Un client A** (dans notre cas la machine cliente fonctionne sous Windows xp)
- **Un authentificateur B (Switch Cisco catalyst).**
- **Un serveur d'authentification C (**Le serveur Radius IAS sous Windows server 2003).

L'utilisateur (Client A) désire accéder à des ressources partagées du réseau local via un port d'authentificateur (Switch capable de faire 802.1x), pour cela le demandeur (Client A) demande à s'authentifier via le commutateur avant de pouvoir accéder aux ressources du réseau. Celui-ci laissera passer ou non le trafic de réseau selon la réponse de serveur d'authentification (RADIUS), qui vas autoriser l'authentification à fournir, ou non le service au client. Comme il est illustré dans la figure suivante.

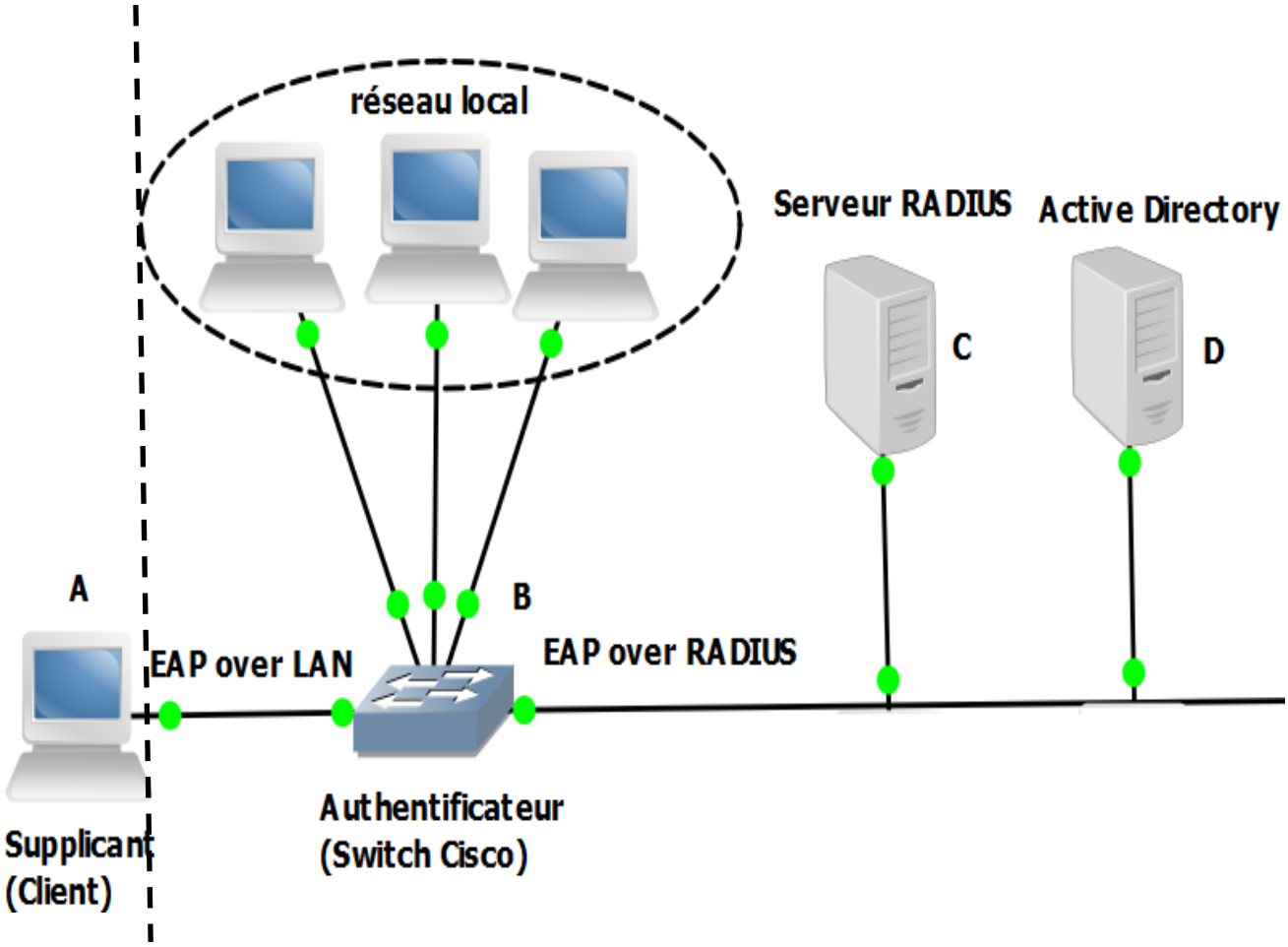


Figure V.1 : Infrastructure permettant une authentification **802.1x**

V.3 Explication de l'infrastructure permettant une authentification 802.1x :

L'utilisateur (Client A) veut se connecter au réseau local via un port d'un commutateur capable de faire l'authentification **802.1x,** pour cela le Client (A) demande à s'authentifier en envoyant des échanges d'informations spécifiques (login, mot passe…),qui sont appelés flux EAPOL (EAP over LAN) à travers le port non contrôlé (uncontrolled) du commutateur qui permet a son tour de les transmettre au serveur d'authentification RADIUS sous forme de EAP over RADIUS. Celui-ci vérifiera si le client a le droit ou non d'accéder au réseau selon les données d'authentifications présentent dans son annuaires (Active Directory). Une fois le client a prouvé son identité, le port contrôlé (controlled) change d'état et devient ouvert et tout le trafic réseau passe par ce port. Si la réponse du serveur d'authentification est négative, le port reste bloqué dans son état initial. Mais le processus d'authentification peut être retenté plusieurs fois. Au bout d'un nombre d'essais défini, l'authentification échoue et l'accès au réseau est bloqué.

Notons que:

1. quand un client configuré avec le protocole **802.1X** se connecte à un commutateur qui n'a pas d'authentification activée, le client va tenter de s'authentifier en envoyant une première requête EAPOL. Ne recevant pas de réponse, il va retenter plusieurs fois avant « d'abandonner » et de considérer le port comme étant dans l'état « contrôlé » et ainsi envoyer tout le trafic réseau.

2. Lorsqu'un client se déconnecte, il envoie un message de fin (LOGOFF) qui va permettre au commutateur de passer le port en mode non contrôlé et ainsi attendre l'authentification d'un autre client. Lorsque le lien réseau est coupé, le port va de nouveau demander au client de s'authentifier.

V.4 Configuration des entités :

V.4.1 Le serveur d'authentification Radius (IAS) :

Comme définit dans le chapitre précédent, IAS (Internet Authentication Service) est le Service d'authentification Internet sur Windows server 2003. Il joue le rôle d'intermédiaire entre le serveur d'accès distant et le contrôleur de domaine.

Après avoir installé Windows server 2003 avec les paramètres par défauts quelques modifications s'imposent. En premier lieu il faut s'assurer que le Switch soit capable de reconnaitre le serveur RADIUS IAS, donc on doit attribuer à notre serveur une adresse IP statique et s'assurer que son nom DNS est mis à jour, en envoyant un « ping » au serveur à partir d'un autre ordinateur de réseau. Ensuite on installe Active Directory qui contient les données concernant les différents comptes des utilisateurs de l'entreprise. Ainsi que on installe le service IIS (Internet Information Services), qui est nécessaire à la diffusion de certificats par l'intermédiaire d'une page Web donc il est préférable d'installer IIS avant l'installation de l'autorité de certification.

Une fois l'autorité de certification est installée nous allons générer et installer le certificat pour le serveur d'authentification, et l'exporter avec sa clé privée associée. Puis, on procède à la création d'un compte utilisateur et lui donner un droit d'accès puis on l'associé a un groupe qu'on aura créé, et ceux dans l'annuaire Active Directory et cela pour chaque utilisateur qu'on veut s'authentifier. Et enfin on procède à la configuration du serveur Radius.

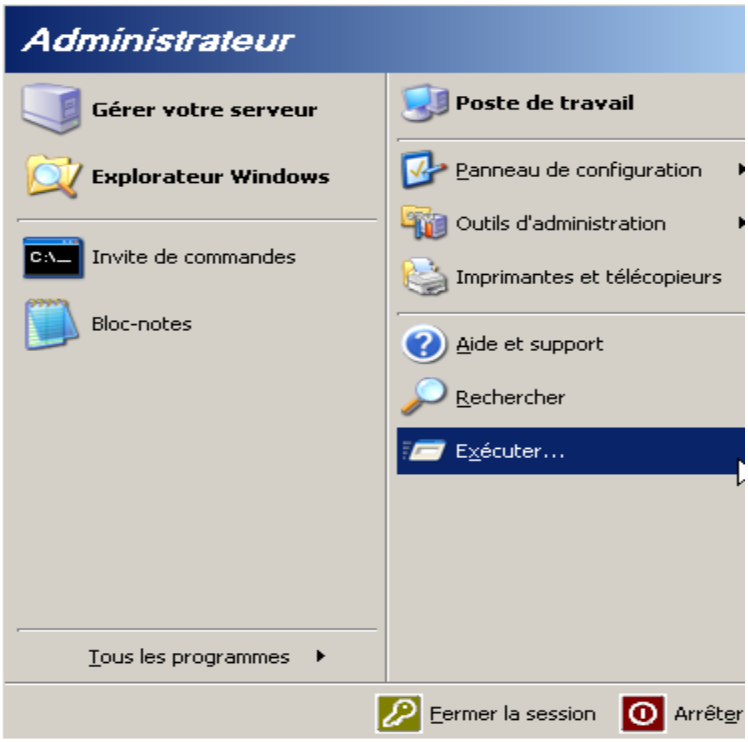
V.4.1.1 L'installation et la gestion d'Active Directory Service :

Deux méthodes sont possibles pour installer Active Directory :

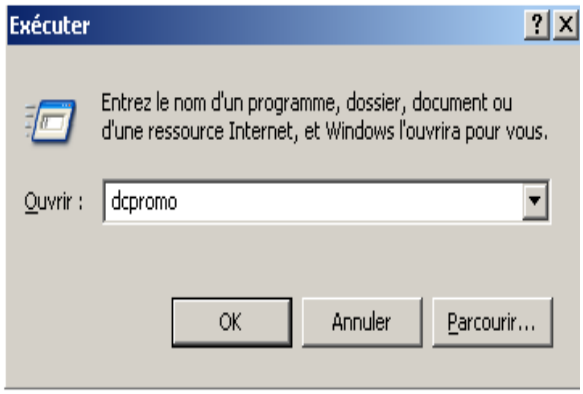
1. Utiliser l'utilitaire « **Gestion de serveur** »
2. Utiliser l'assistant « **dcpromo** »

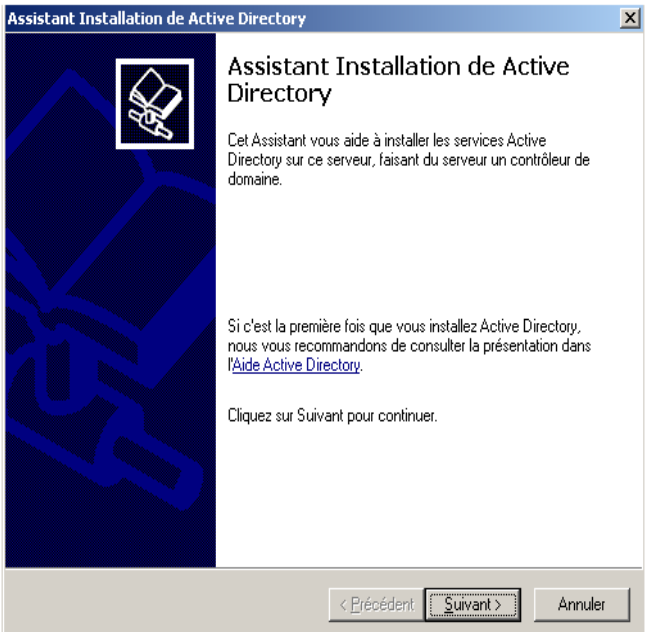
- **Pour installer Active Directory on suit les différentes étapes suivantes :**

On cliquer sur démarrer puis exécuter :

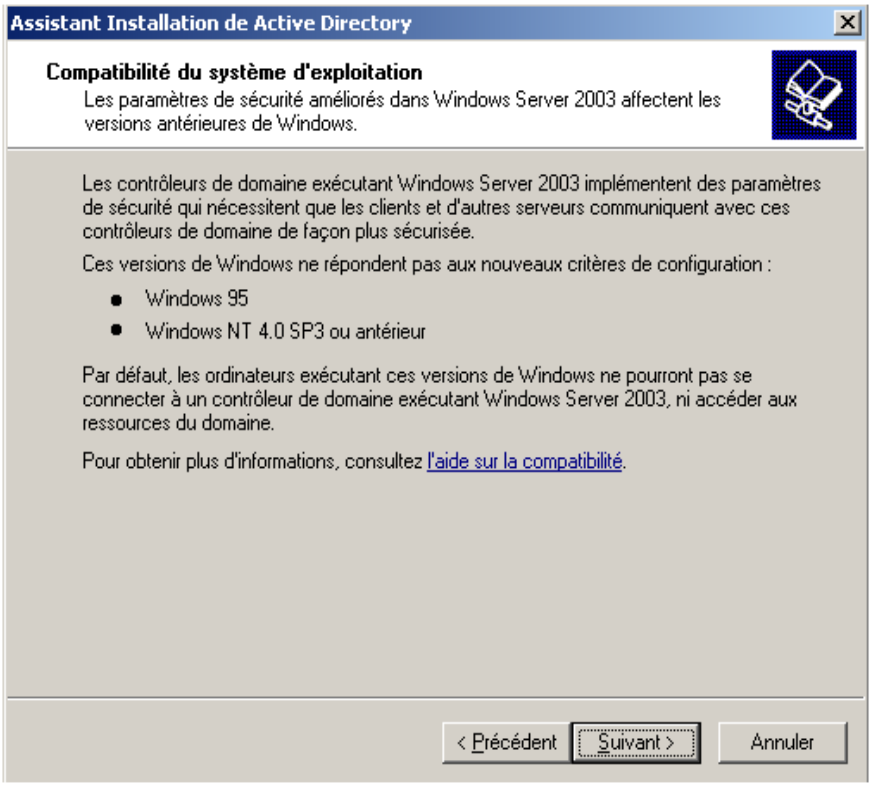


- Exécution de la commande dcpromo, l'assistant de l'installation démarre:

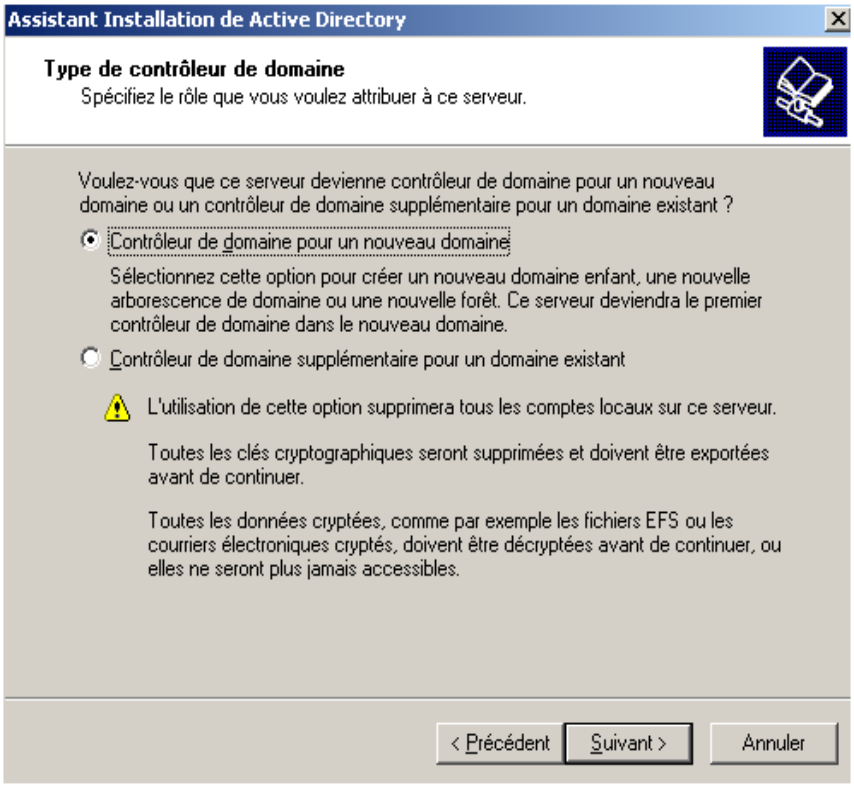




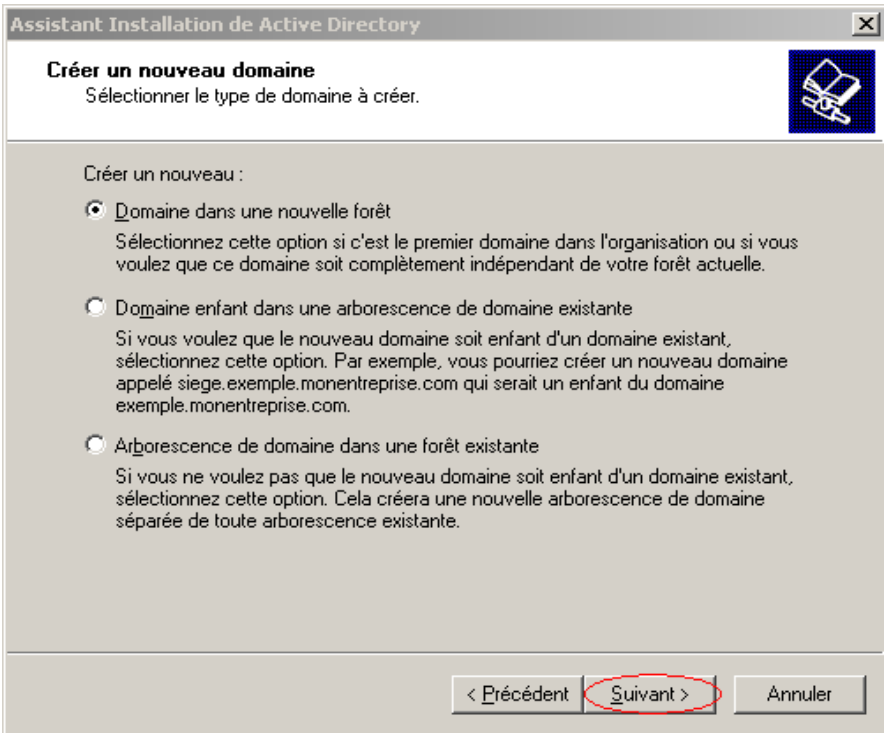
- Dans l'Assistant Configurer votre serveur cliquez sur **suivant**



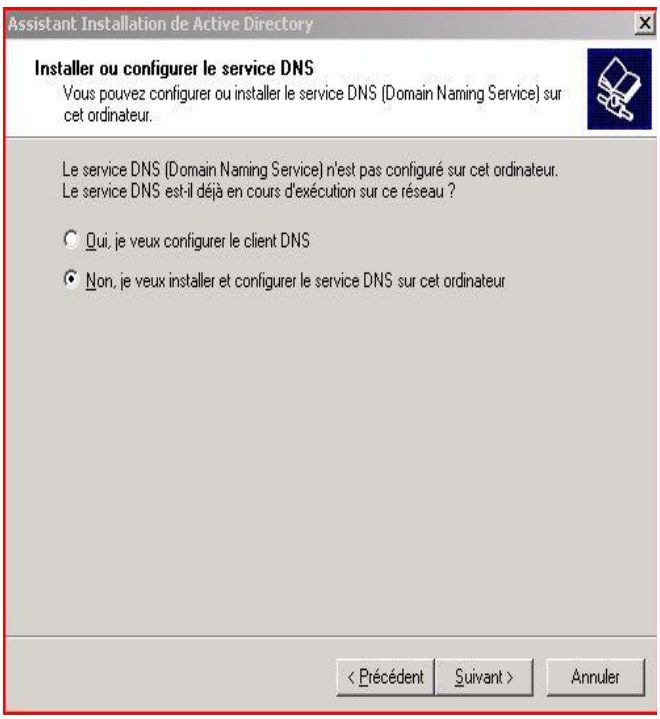
- Sélectionner le type de contrôleur de domaine :

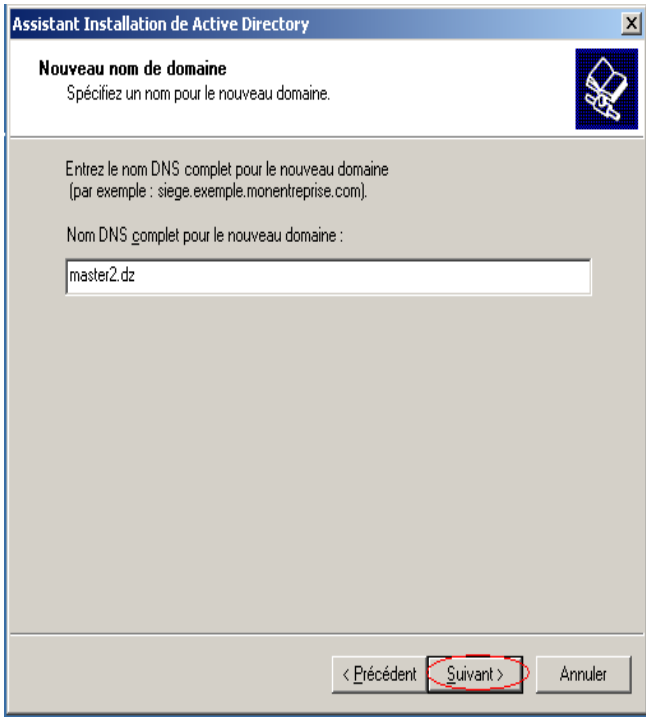


- Sélectionnez le type de domaine **« Domaine dans une nouvelle foret »** puis cliquez sur **Suivant.**

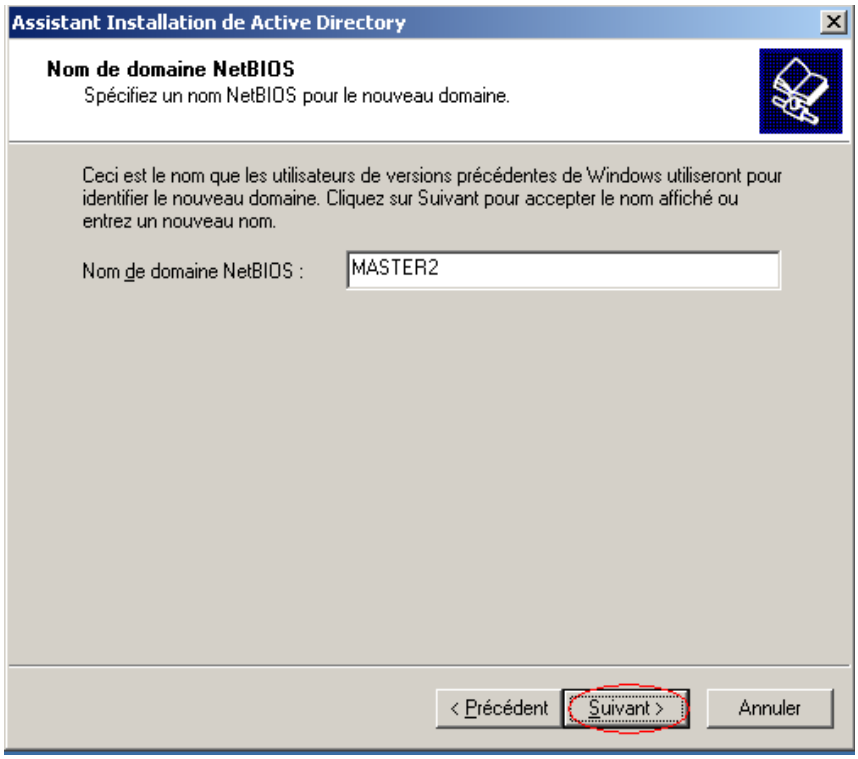


- Cochez « **Non je veux installer et configurer le serveur DNS sur cet ordinateur** » puis cliquez sur **Suivant**, puis spécifiez un nom pour le nom de domaine.

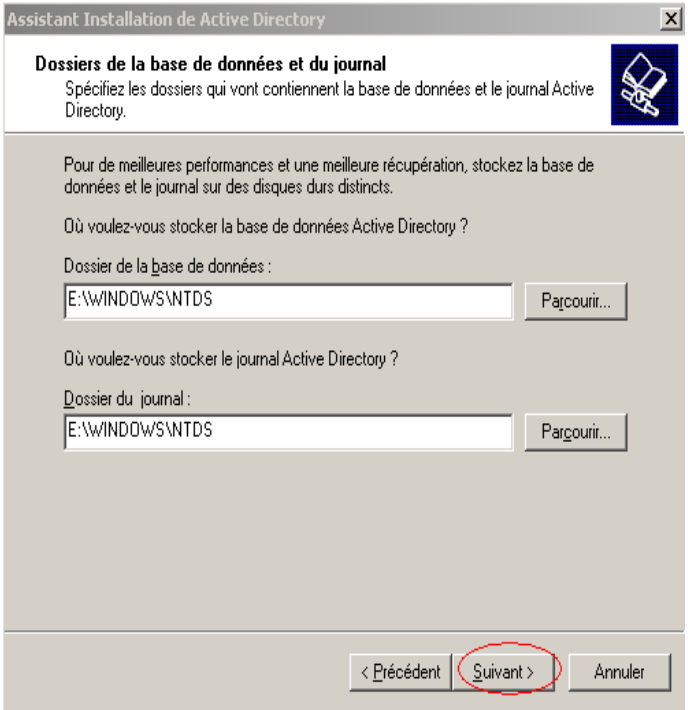


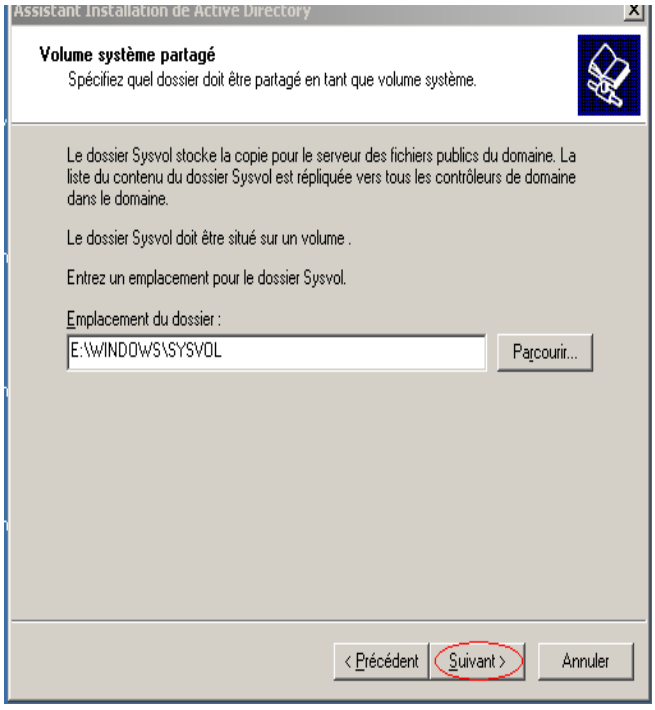


- Spécifiez un nom NetBIOS pour le nouveau domaine puis Suivant :

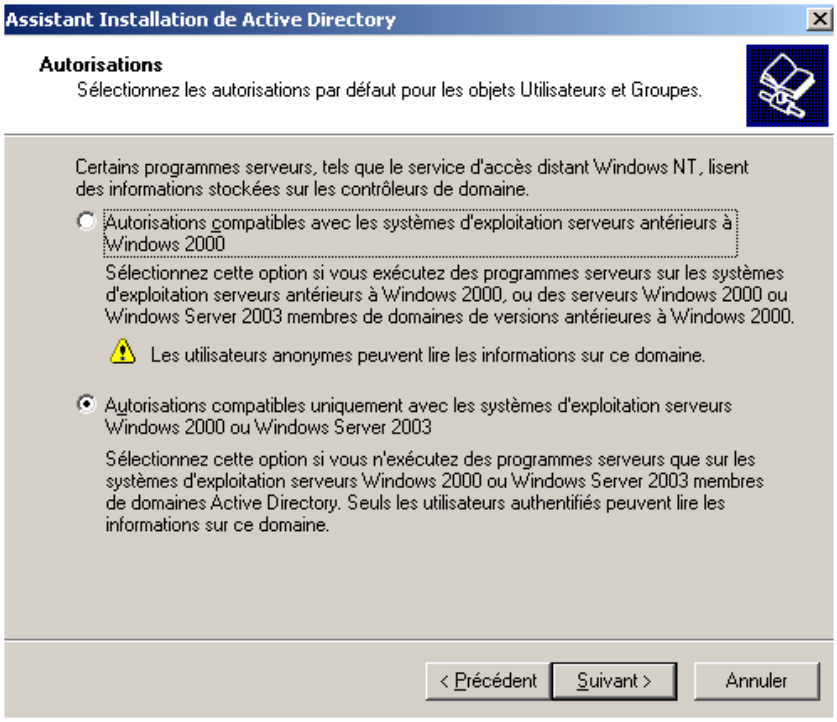


- Ces deux fenêtres permettent de spécifier les dossiers qui vont contiennent la base de données et le journal Active Directory. Puis on clique sur suivant.

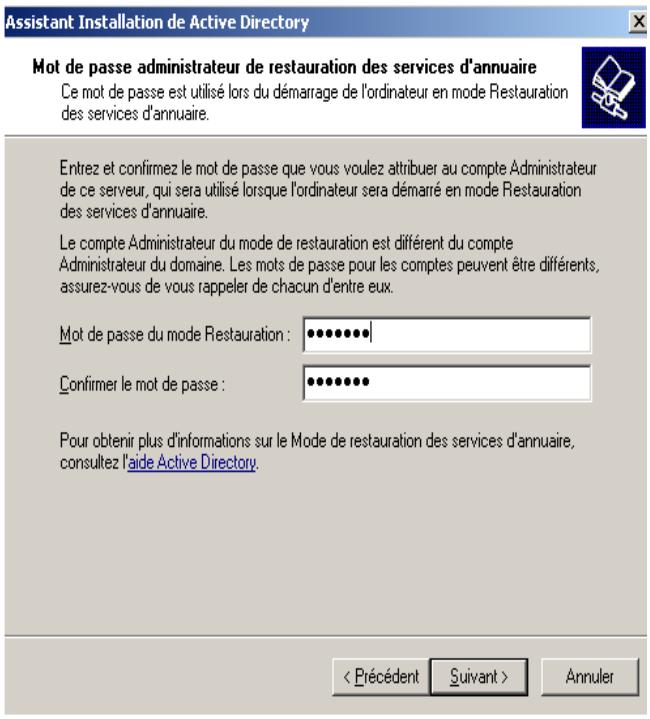


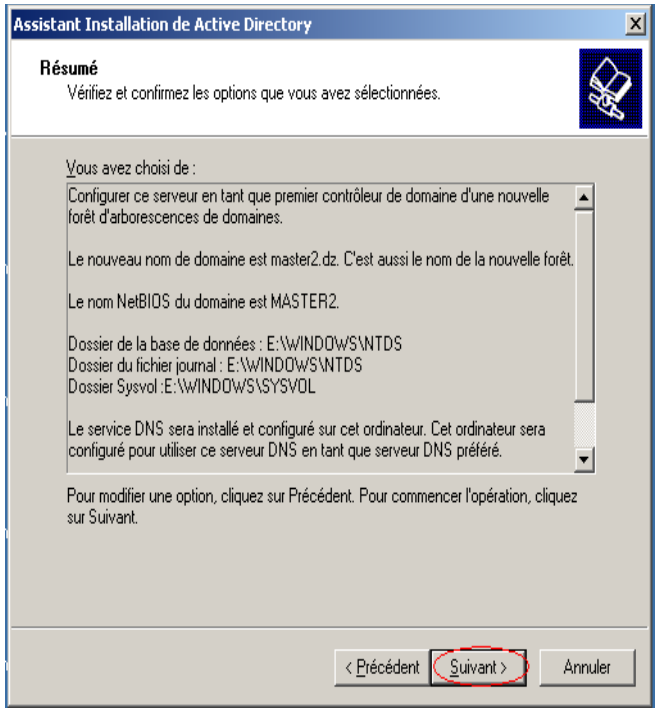


- Sélectionnez les autorisations par défaut pour les objets Utilisateurs et Groupes, puis **suivant.**

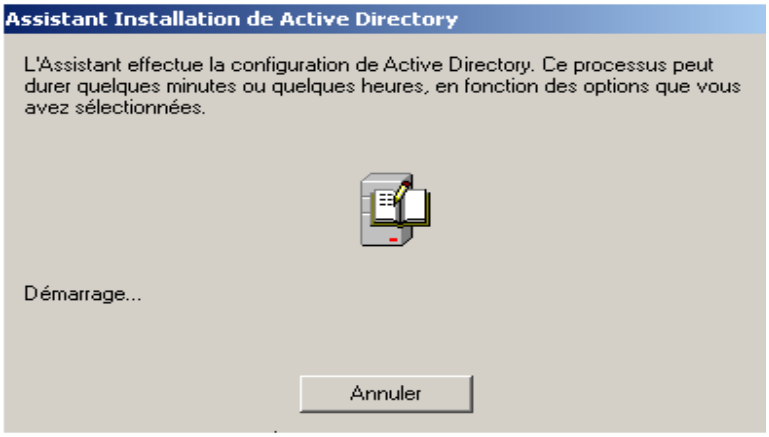


- Créez le mot de passe administrateur de restauration des services d'annuaire et confirmez-le, puis Suivant.

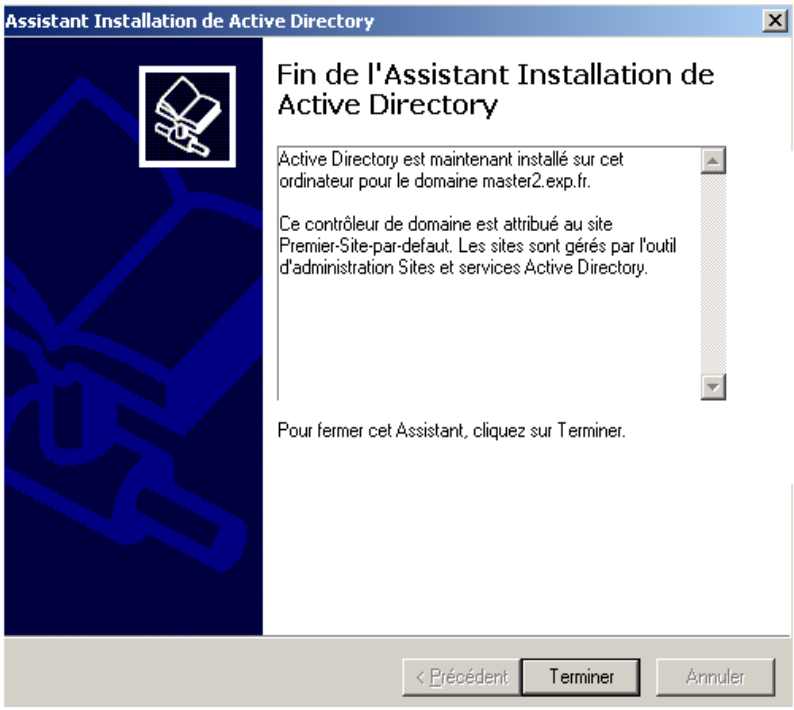


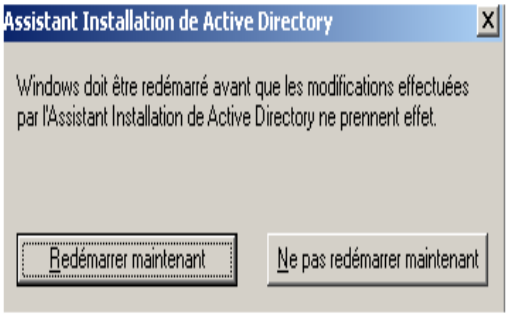


- Démarrage d'Installation d'Active Directory :



- Cliquez sur Terminer pour fermer cet Assistant, puis redémarrer la machine pour prendre en compte les modifications effectuées par l'assistant Active Directory.

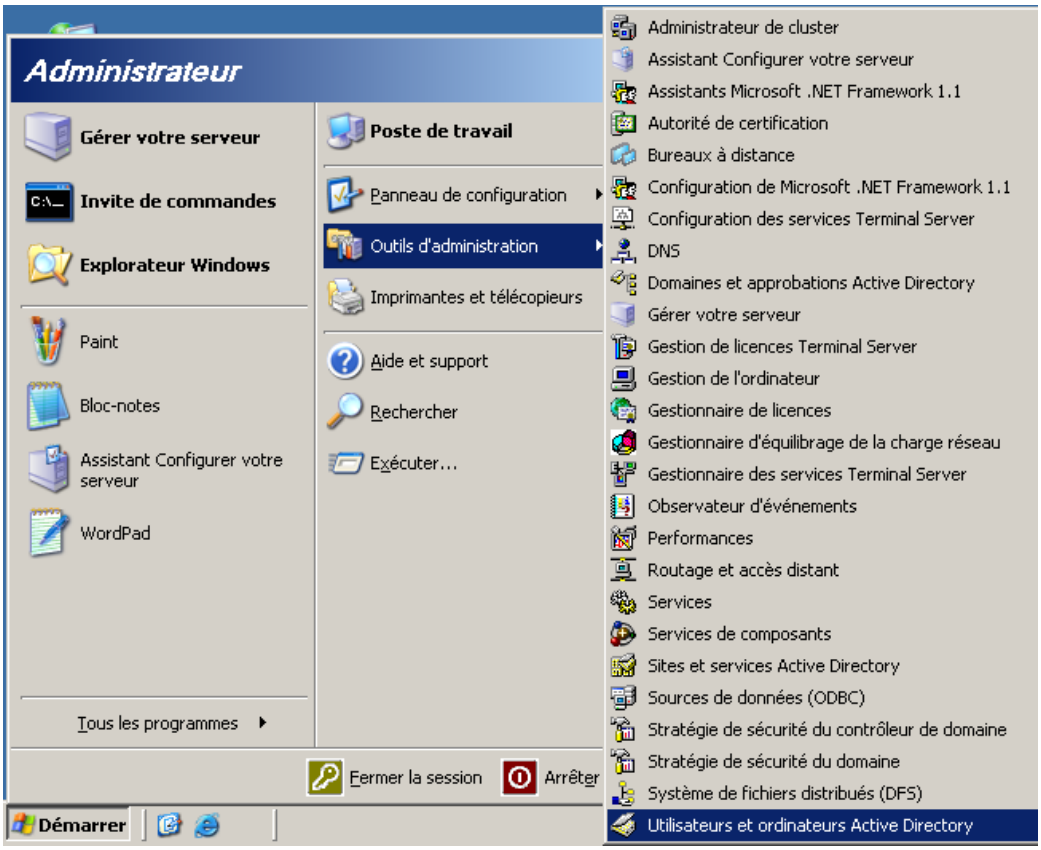




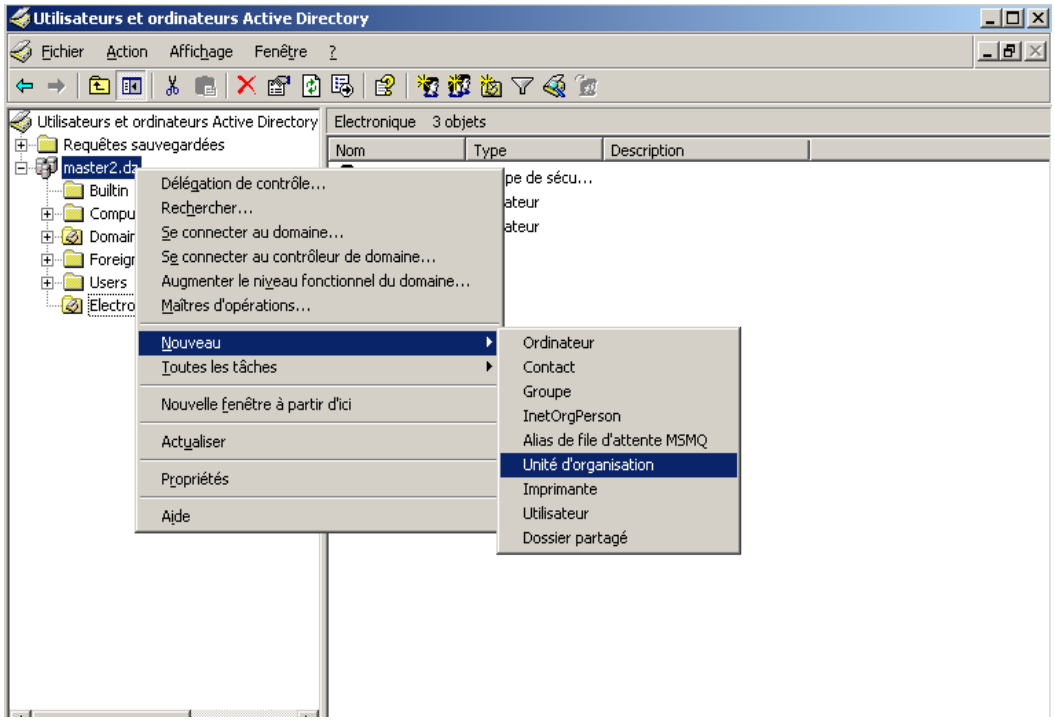
V.4.1.1 .a La création de l'unité d'organisation :

La création d'unité organisationnelle s'effectue par la console Utilisateurs et Ordinateurs Active Directory pour cela **:**

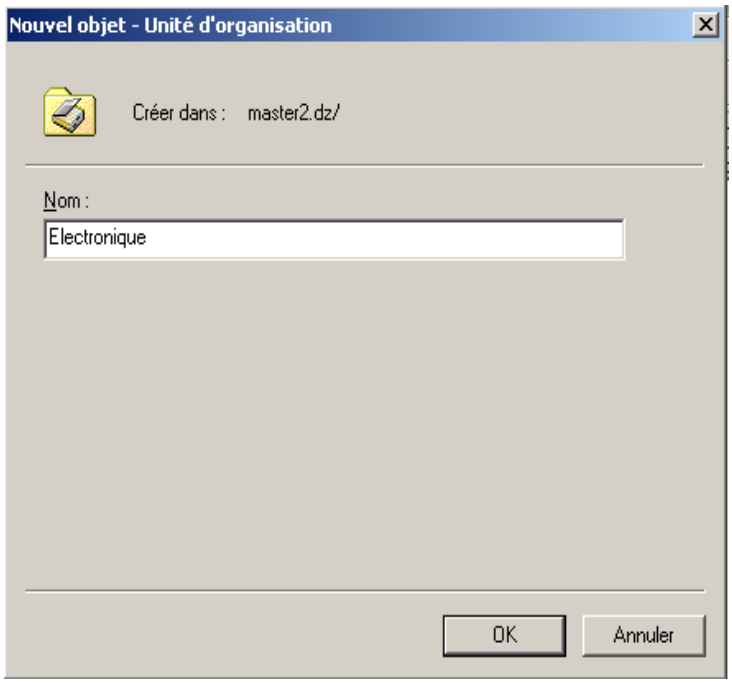
- Cliquez sur **Démarrer –Outils d'administration-Utilisateurs et Ordinateurs Active Directory**



Dans le volet de gauche, cliquez de droit sur votre Nom de domaine puis pointez sur « **Nouveau** » et cliquez sur « **unité d'organisation** ».

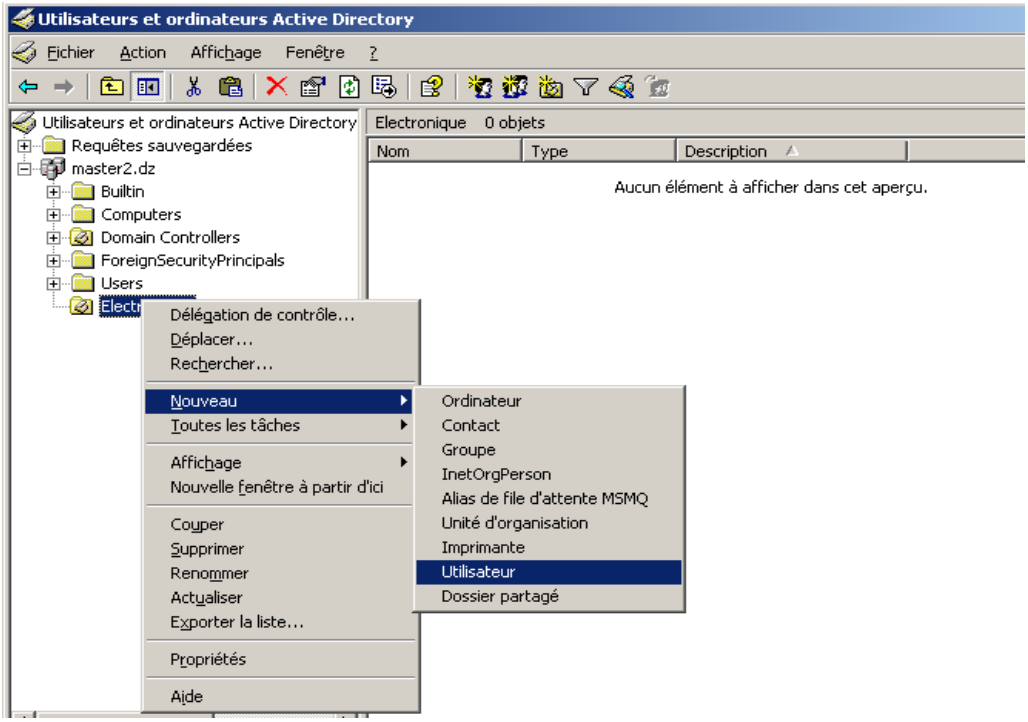


Tapez «**Electronique**» dans la zone de Nom, puis cliquez sur « **OK** ».



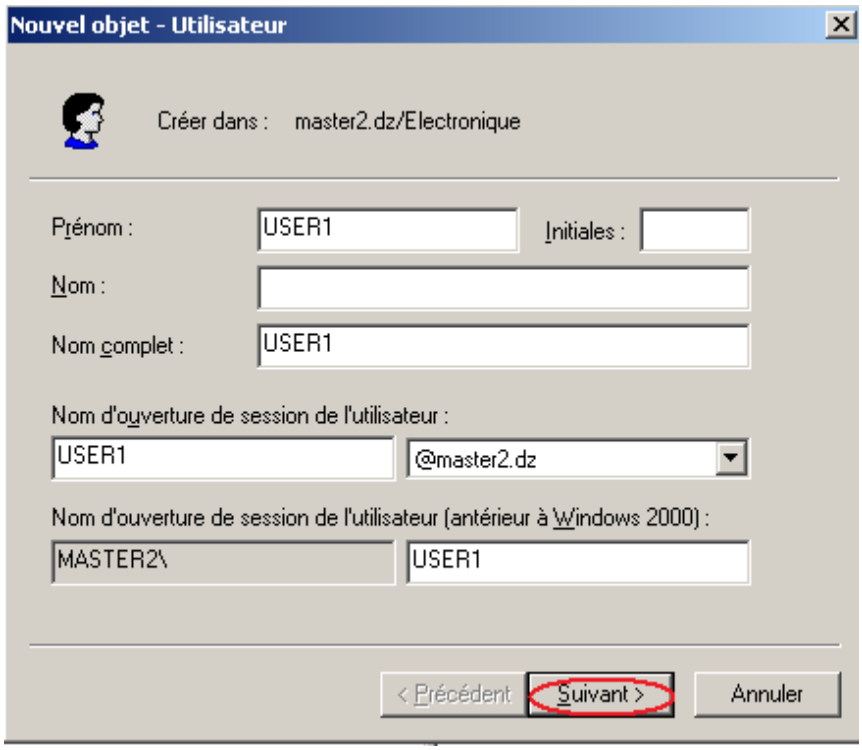
V.4.1.1 .b Création d'un compte d'utilisateur et d'un groupe dans Active Directory :

Dans un dossier «**Electronique**», faites un clique droit avec la souris puis un nouveau utilisateur.

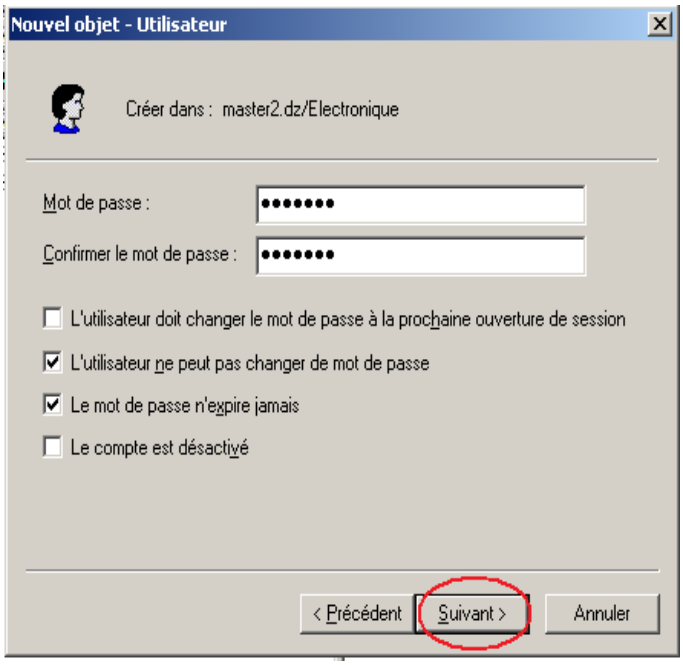


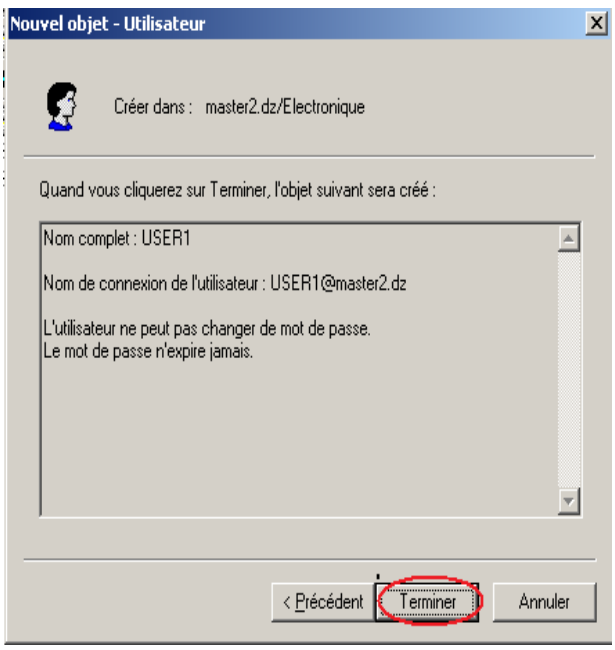
Remplissez les zones **« Nom »** et **« Prénom »** comme vous le chosiez et notez que

ceux-ci s'affichent automatiquement dans la zone « **Nom complet** ». Remplissez ensuite la zone **« Nom d'ouverture de session d'utilisateur ».**

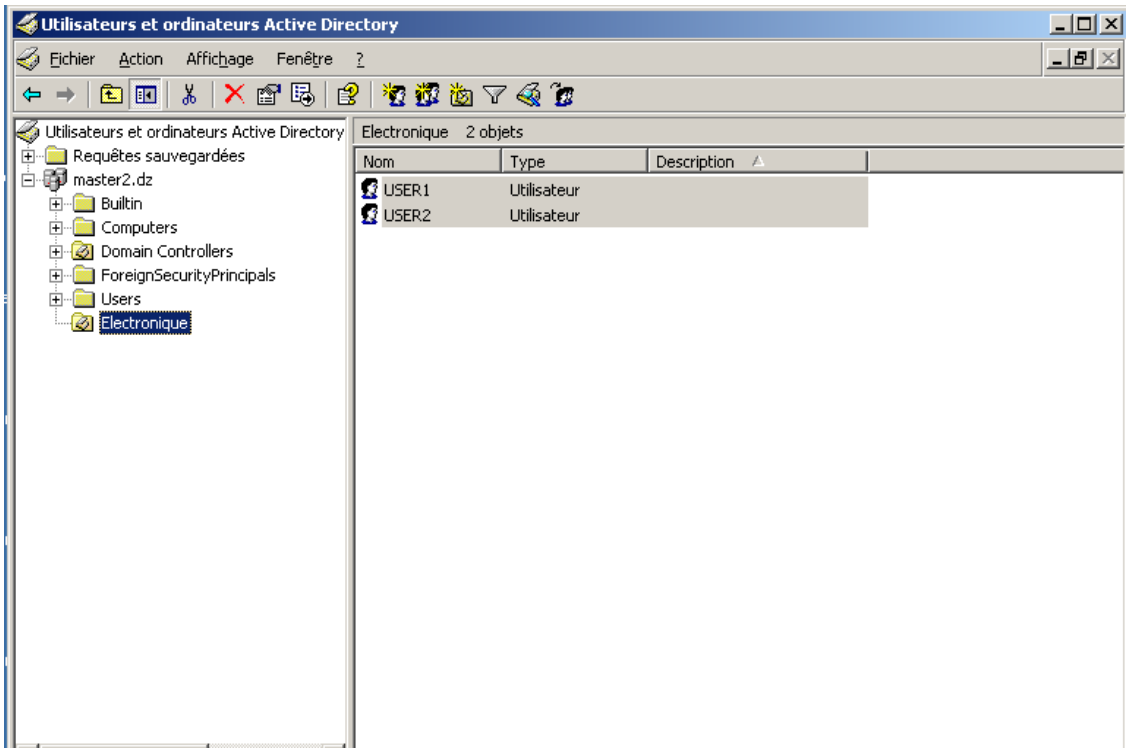


Entrez ensuite le mot de passe dans les zones **« Mot de passe »** ainsi que les options concernant le compte, Puis sur terminé.

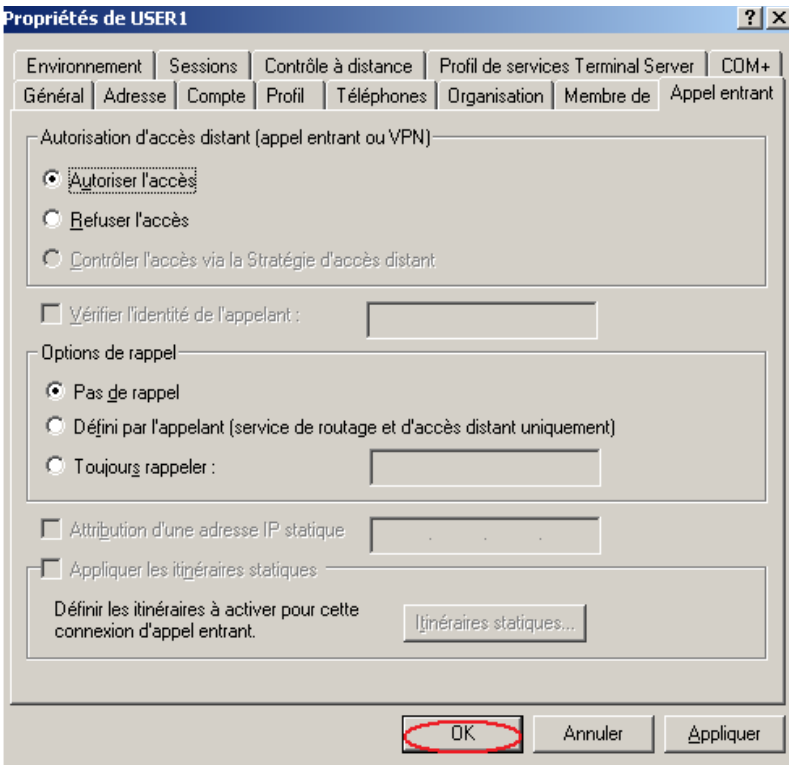




Tous les utilisateurs crées seront affichés dans le volet droite comme le montre la fenêtre suivante :

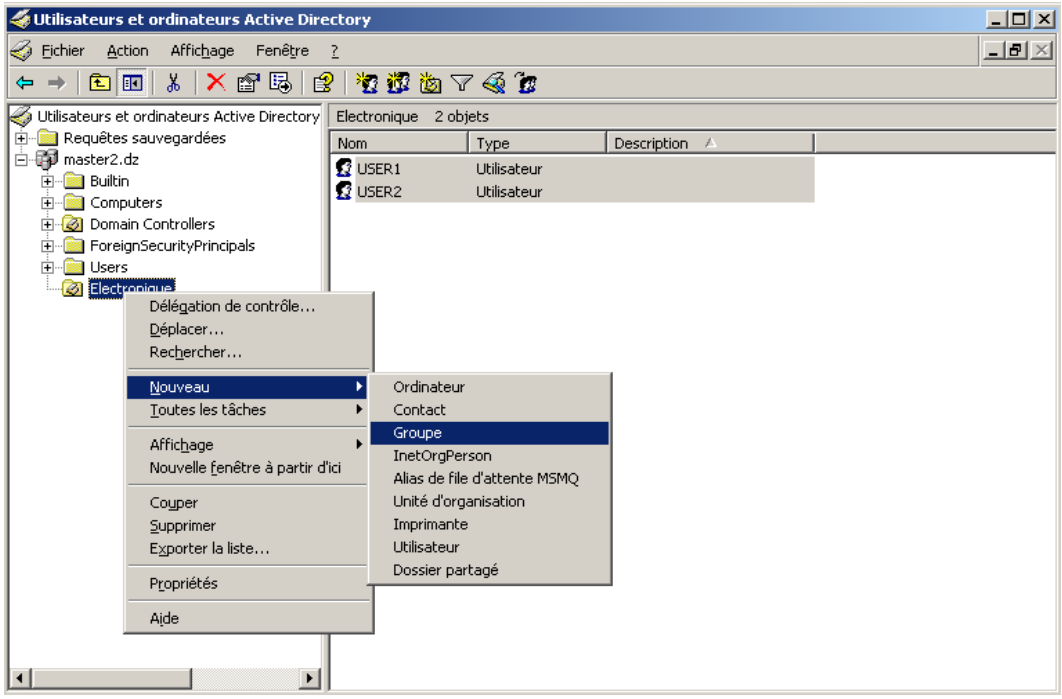


Ensuite, on édite les propriétés du client (USER1 par exemple) pour autoriser l'accès distant en sélectionnant Autorisé l'accès dans la section Autorisation d'accès distant sous l'onglet Appel entrant et on valide par **OK.**

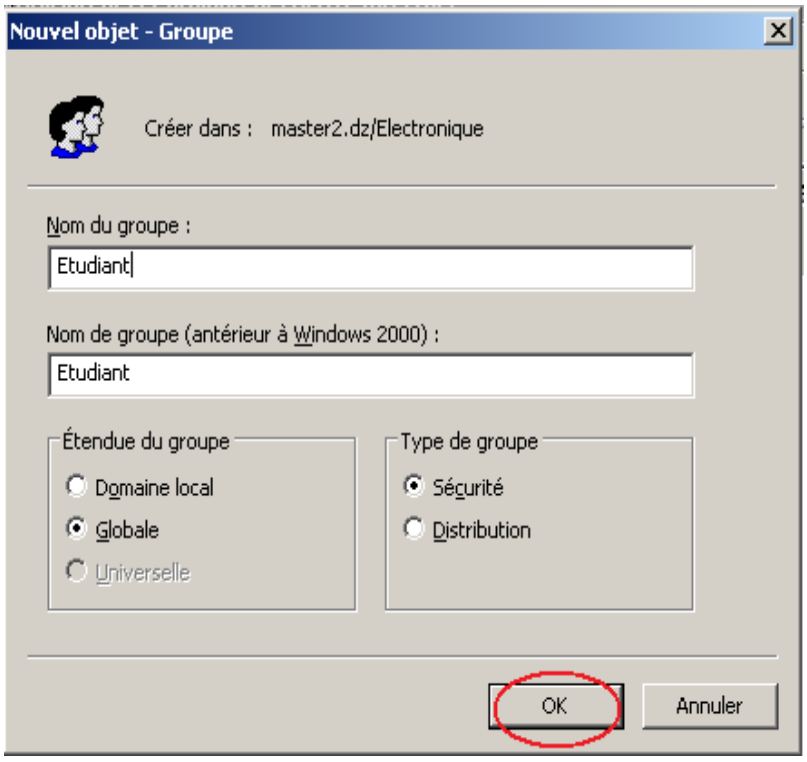


V.4.1.1 .c Création d'un groupe d'utilisateur (groupe de sécurité):

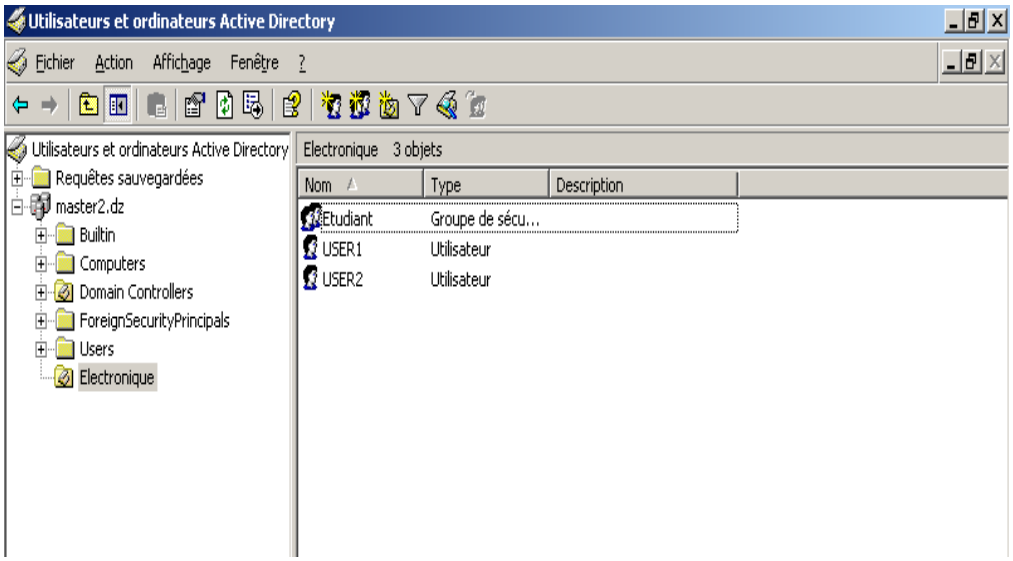
Nous pouvons maintenant créer un groupe d'utilisateurs qui contiendra les utilisateurs, dans le dossier Electronique faites un click droit puis nouveau groupe que l'on appellera « **Etudiant** ».



Dans la boite de dialogue **Nouvel Objet-Groupe**, entrez le Nom du groupe **« Etudiant »**



Dans la fenêtre apparue il affiche le groupe crée :

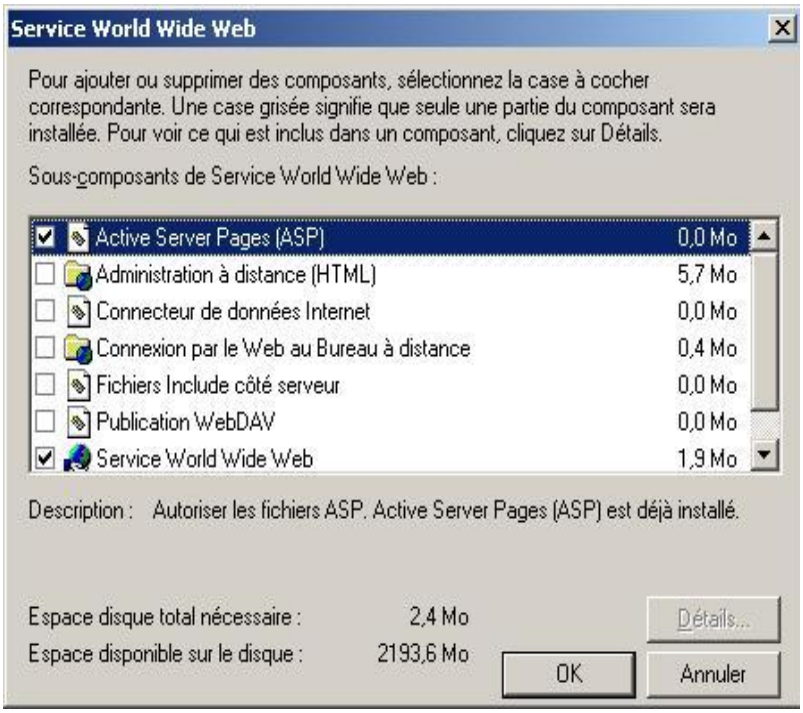


V.4.1.2 Installation de service Certificat :

Si vous envisagez la diffusion de certificats par l'intermédiaire d'une page Web, il est préférable d'installer IIS (Internet Information Services) avant l'installation de l'autorité de certification. De cette manière, IIS sera automatiquement configuré pour diffuser des certificats.

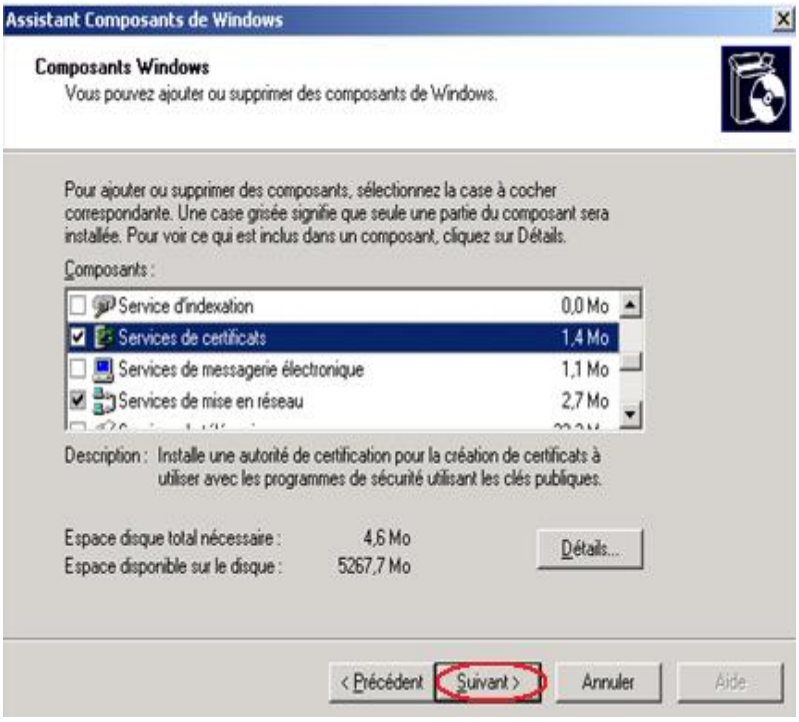
i. Premièrement installation d'IIS (Internet Information Service) :

Pour installer IIS, il faut aller vers « **Ajout/Suppression de programmes** » dans le panneau de configuration. Sélectionnez « **Ajouter ou supprimer des composants Windows** », double cliquez sur « **Serveur d'applications** », sur « **Services IIS** » puis sur « **Services World Wide Web** ». Sur la fenêtre qui s'ouvre, cochez « **Active Server Pages (ASP)** » ainsi que « **Services World Wide Web** » puis cliquez sur le bouton **OK**. Lancez l'installation à l'aide du bouton **Suivant**.

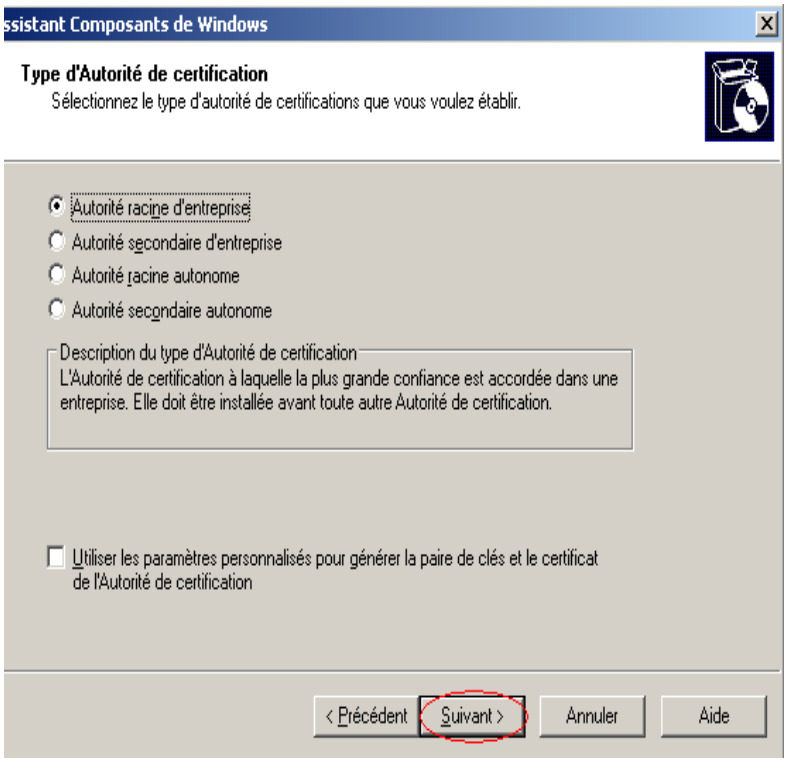


ii. Deuxièmement installation des services de certificat :

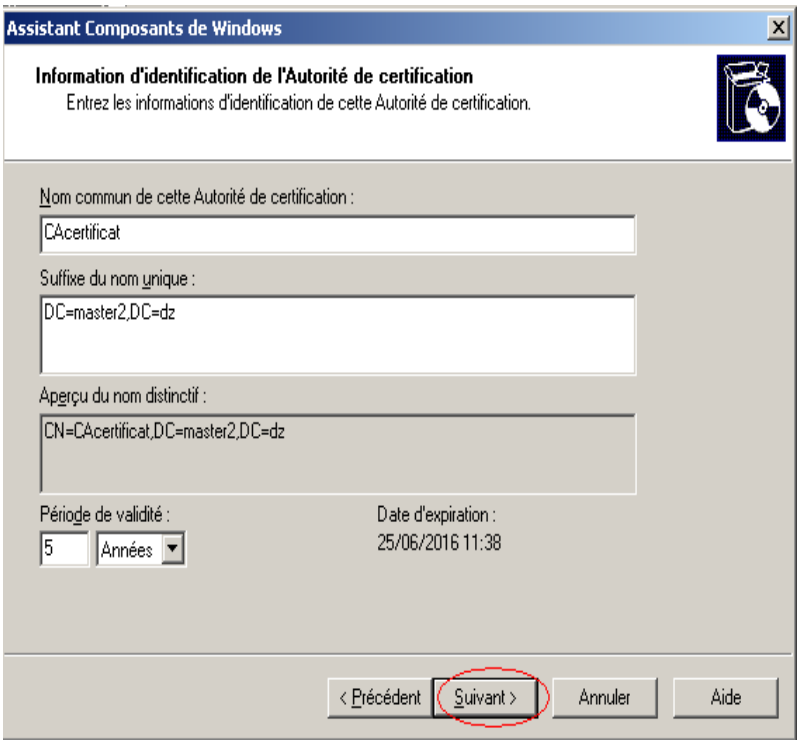
Après l'installation des services de certificats, il n'est plus possible de changer le nom ou le domaine du serveur. Pour installer une autorité de certification sous Windows Server 2003, il faut se rendre dans « **Ajout/Suppression de programmes** » dans le panneau de configuration. Sélectionnez « **Ajouter ou supprimer des composants Windows** », cochez « **Services de certificats** » puis cliquez sur le bouton « **Suivan**t ».



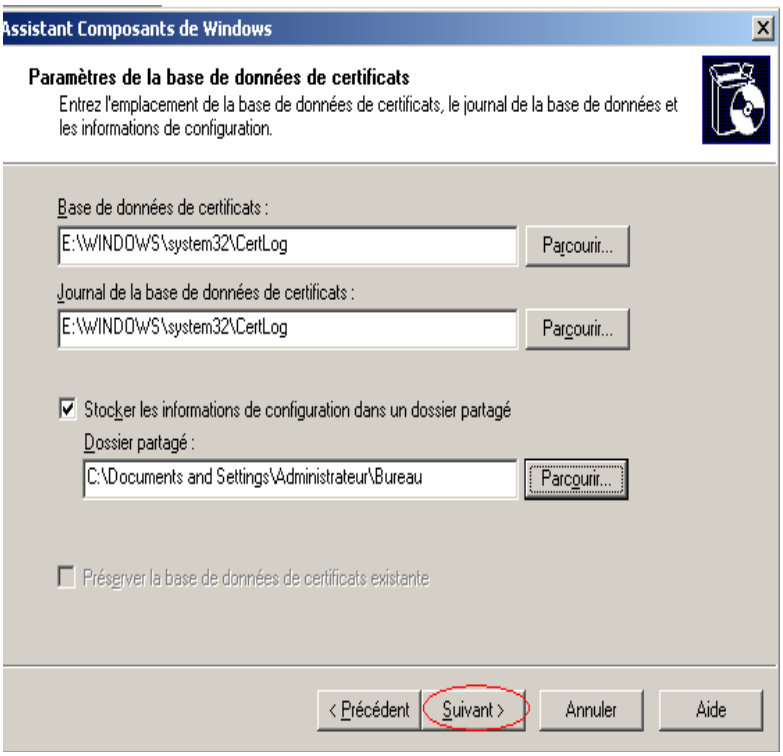
La première étape de l'installation consiste à choisir le type d'autorité de certification.



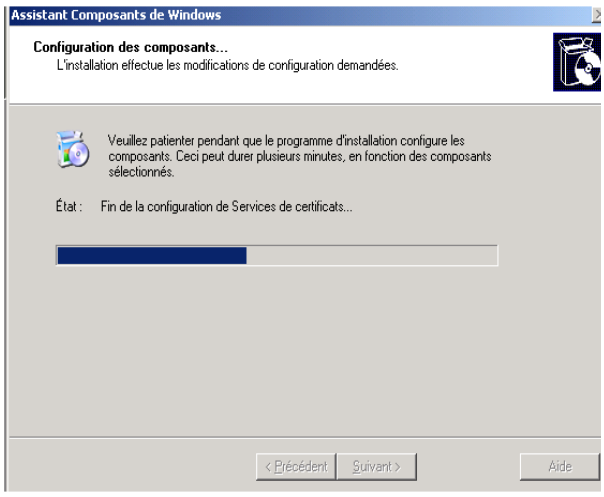
Il faut ensuite choisir un nom pour cette autorité de certification ainsi que, dans le cas d'une autorité racine, la période de validité des certificats délivrés.



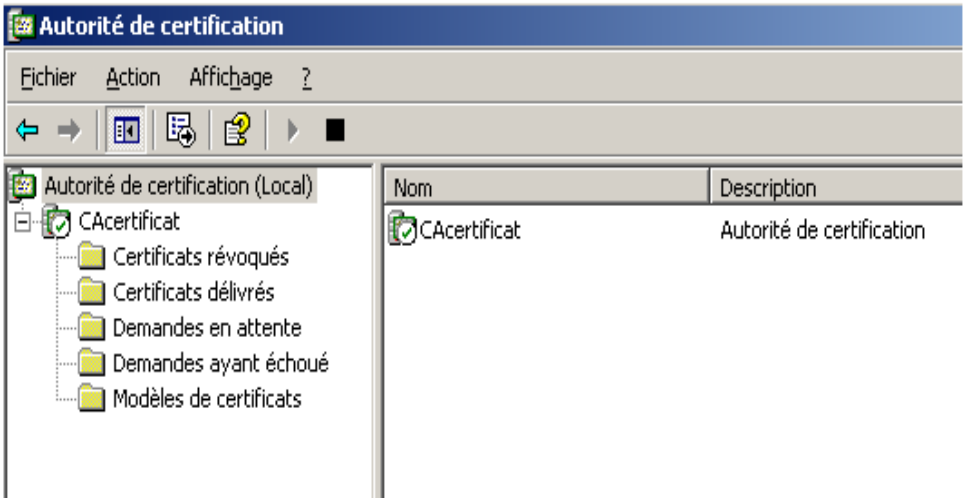
Pour terminer l'installation propose de changer l'emplacement de la base des certificats et des fichiers journaux



Après avoir validé cette dernière étape, la copie des fichiers nécessaires commence.

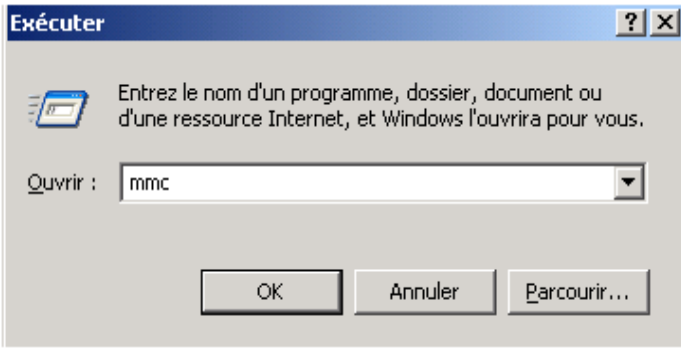


Une fois l'installation effectuée, un nouveau composant apparait dans le menu « Outils d'administration » de Windows server 2003 **''Autorité de certification''**, qui permet de gérer les autorité de certification.

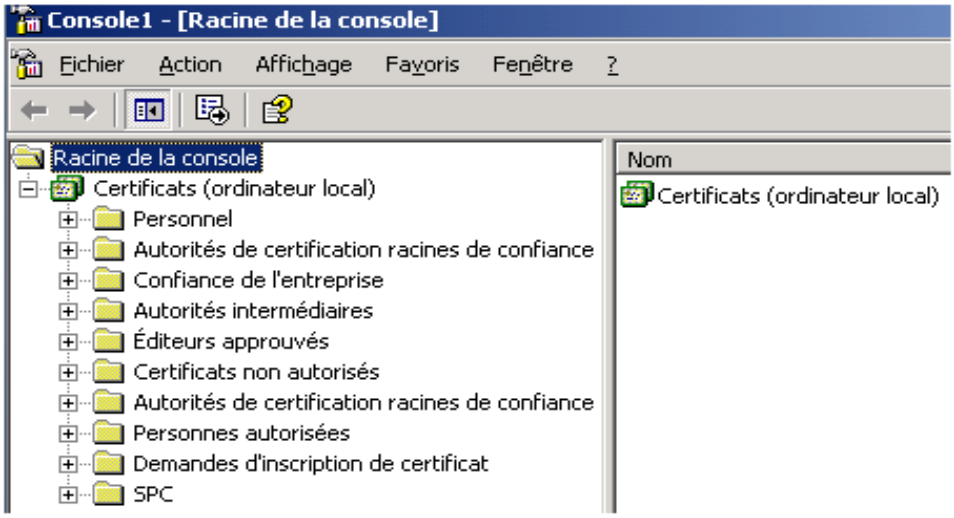


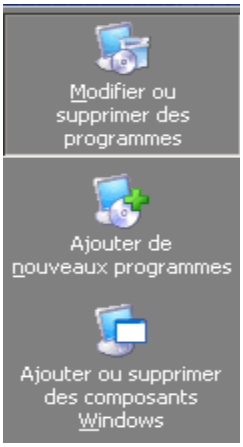
iii. Troisièmement installation de la MMC certificats (l'Autorité racine) :

Le composant enfichable Certificats permet de gérer les certificats d'un utilisateur ou d'un ordinateur. Pour cela, dans le **menu démarre**r, choisissez « **Exécuter** » puis entrez « **MMC** ».



Dans la fenêtre qui s'ouvre, déroulez le menu « Fichier » puis choisissez « **Ajouter/Supprimer un composant logiciel enfichable** ». Sélectionnez le bouton « **Ajouter** » puis double cliquez sur « **Certificats** ». Vous pouvez alors choisir d'afficher les certificats de l'utilisateur actuel ou alors de l'ordinateur.



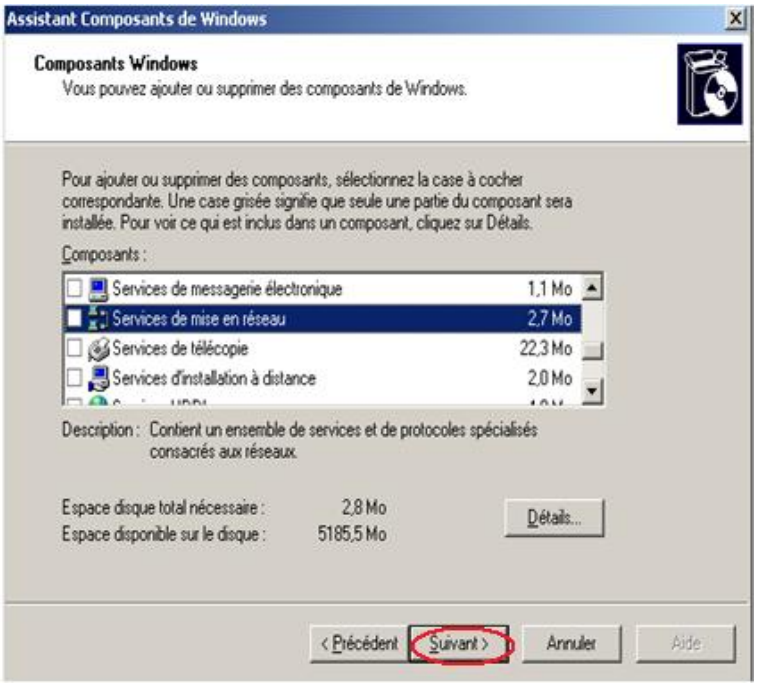


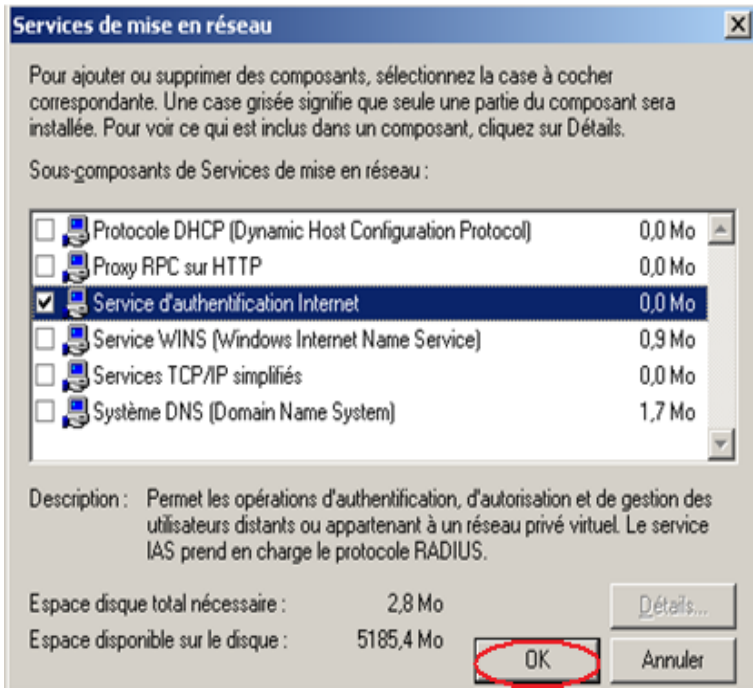
V.4.1.3 Installation et configuration de serveur Radius (IAS) :

V.4.1.3.a Installation d'ISA SERVEUR :

Pour lancer l'installation du service IAS, allez dans le panneau de configuration, puis sélectionnez ajout/suppression des programmes.
Cliquez ensuite sur le bouton Ajouter ou supprimer des composants de Windows.

Dans la première fenêtre de l'assistant Composants de Windows, sélectionnez Services de mise en réseau, puis dans « **Détails** » il faut cocher Service d'authentification Internet



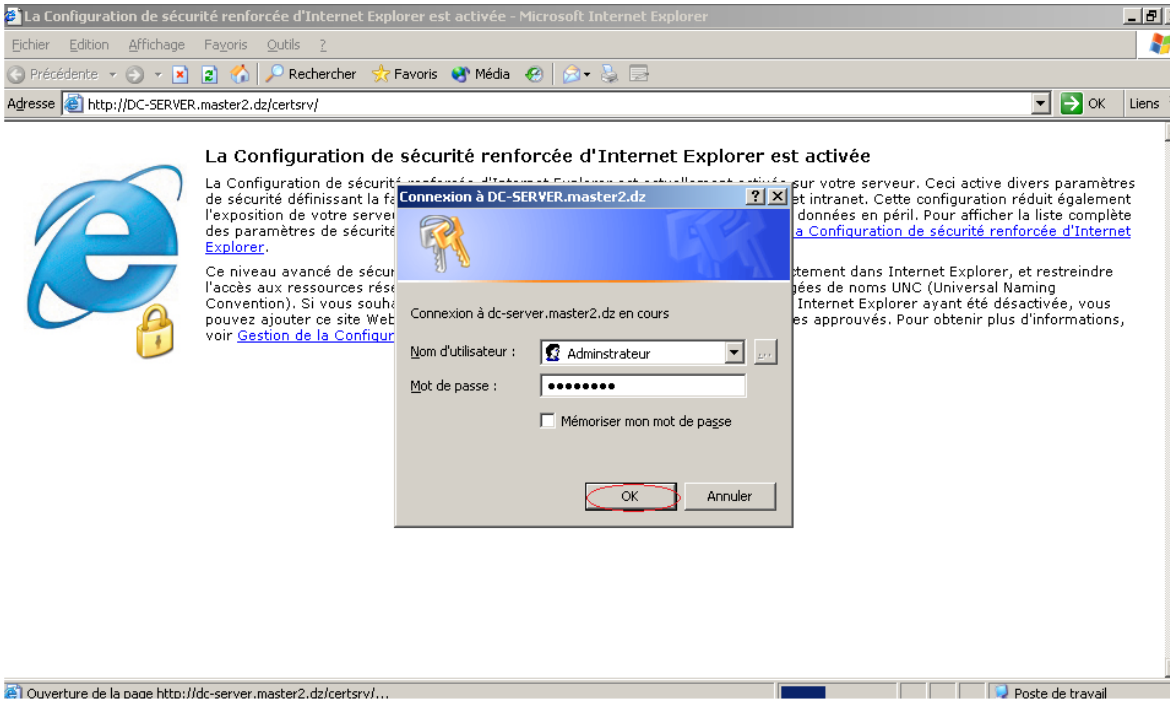


Une fois le service installé, vous pouvez y accéder en tapant **ias.msc** dans la boite de dialogue « exécuter » ou bien en cliquant sur Service d'authentification Internet dans outils d'administration.

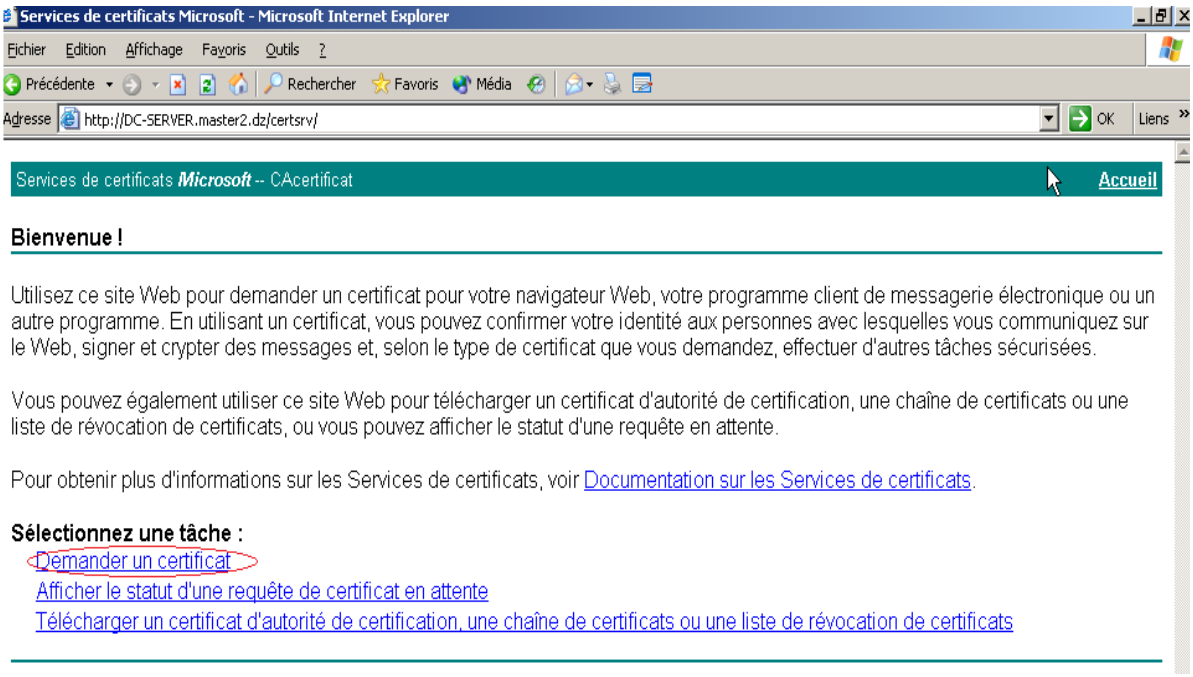
i. Génération et installation d'un certificat X509 pour le serveur Radius IAS :

i.1 Génération d'un certificat X509 :

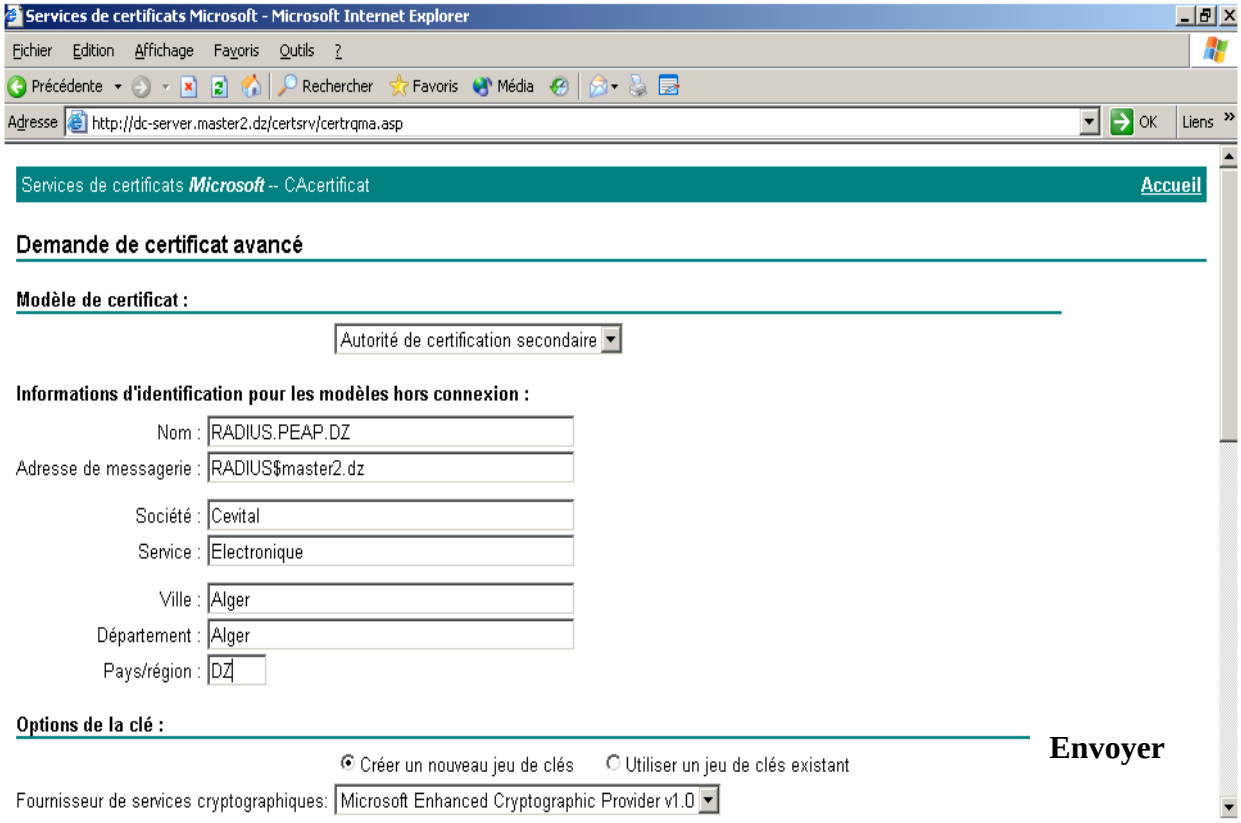
Ce certificat permet d'établir une connexion SSL (Secure Sockets Layer) entre la station de travail (Client) et le serveur Radius. Pour effectuer une demande de certificat on se connecte à l'aide d'Internet Explorer sur le site http://127.0.01/certsrv/ ou bien http://DC-SERVER.master2.dz/certsvr/ ,la fenêtre suivante apparait :



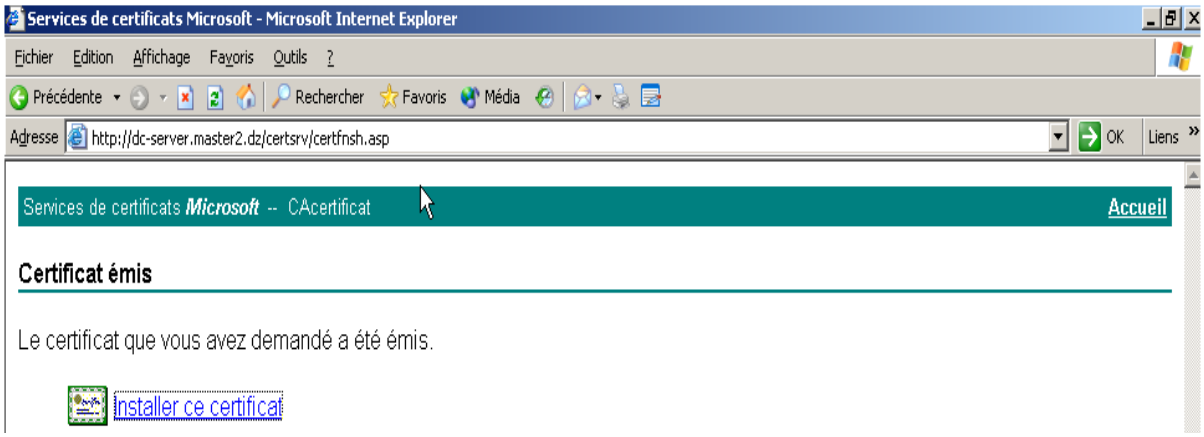
On choisit l'option Demande un certificat :



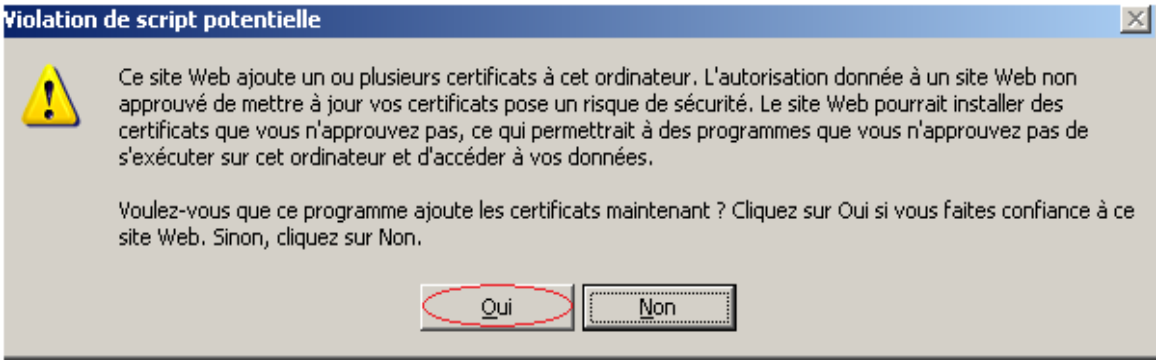
Puis, **Demande de certificat avancée** dans la fenêtre qui s'affiche sélectionnez : **Créer et soumettre une demande de requête auprès de cette Autorité de certification.** On continue à remplir les informations d'identification :



Un avertissement apparait. On conforme la demande du certificat donc le certificat demandé est émis



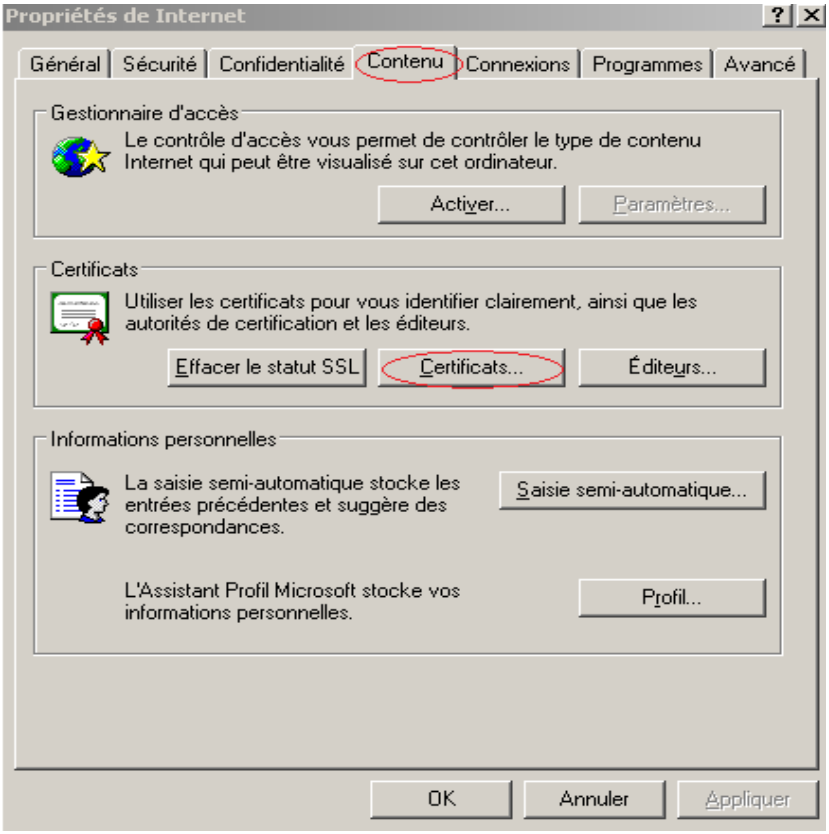
- On cliquant sur installer ce certificat le message suivant s'affiche :



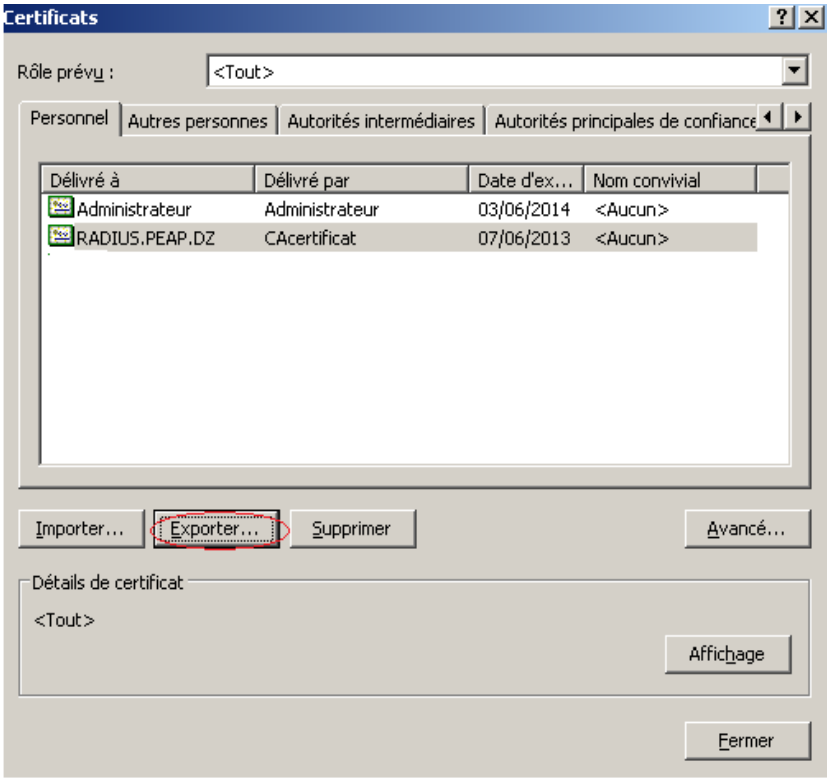
Après la confirmation du message, le certificat est installé correctement.

Donc il nous reste à **exporter** ce certificat et sa clé privée associée via Internet Explorer. Et pour cela on procède comme suit :

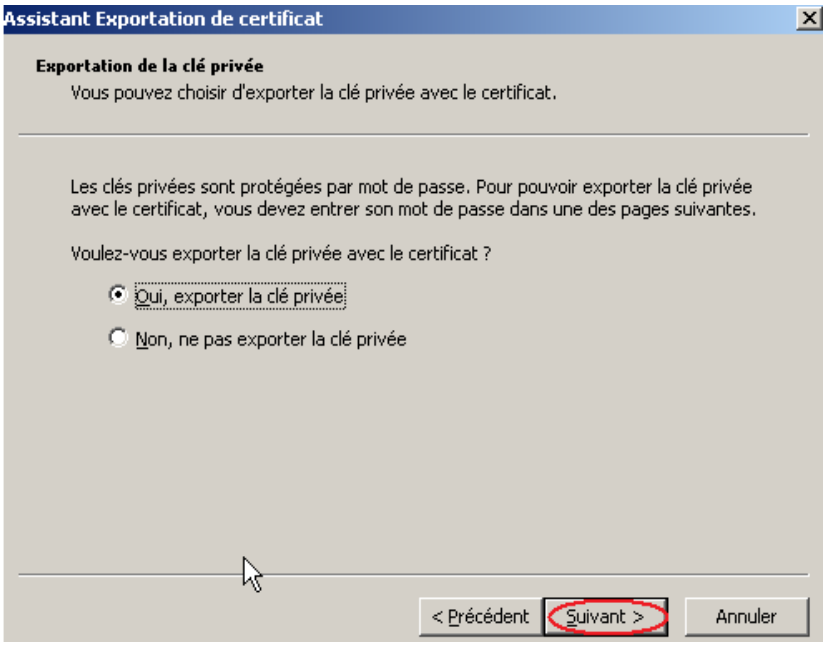
- Cliquez sur Démarrer, cliquez sur Panneau de configuration, puis cliquez sur Option Internet.
- Sous l'onglet Contenus, cliquez sur l'icône certificat



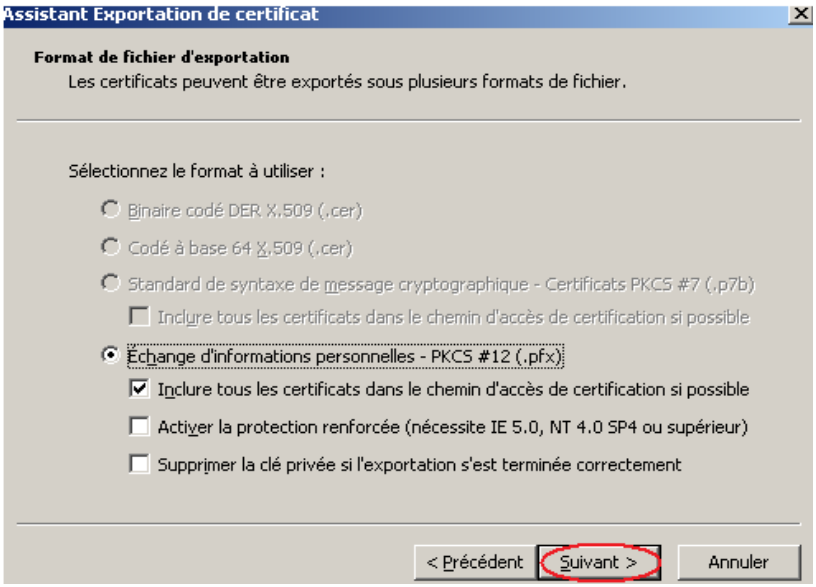
On sélectionne le certificat crée précédemment « **RADIUS.PEAP.DZ** », puis on l'exporte en appuyant sur Exporter.



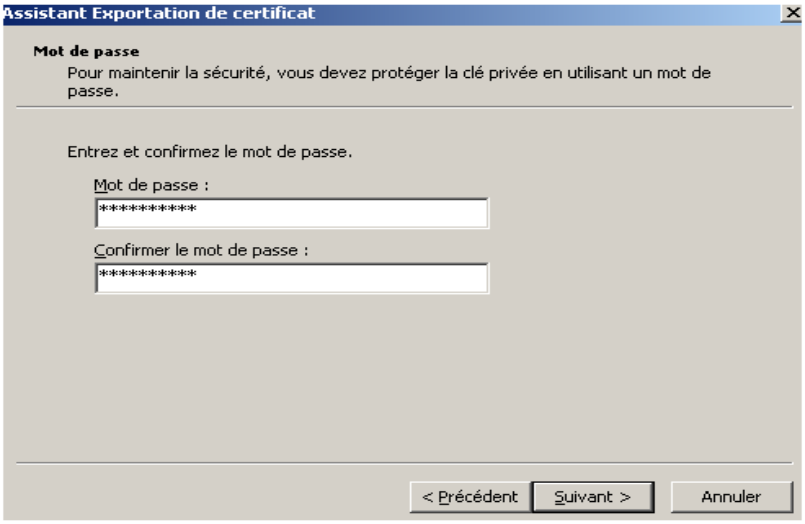
Dans la fenêtre qui apparait on coche la case « oui, exporté la clé privé »:



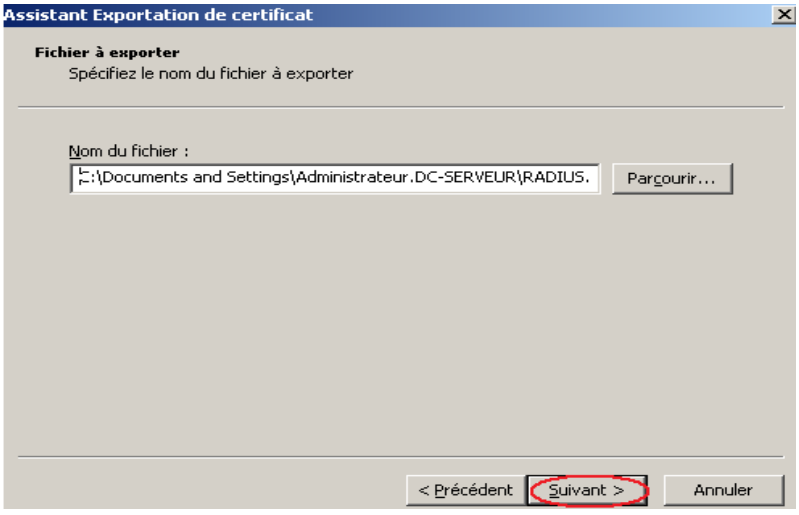
Sélectionnez le format de fichier d'exportation :



Pour maintenir la sécurité, on protège la clé privée en utilisant un mot de passe.



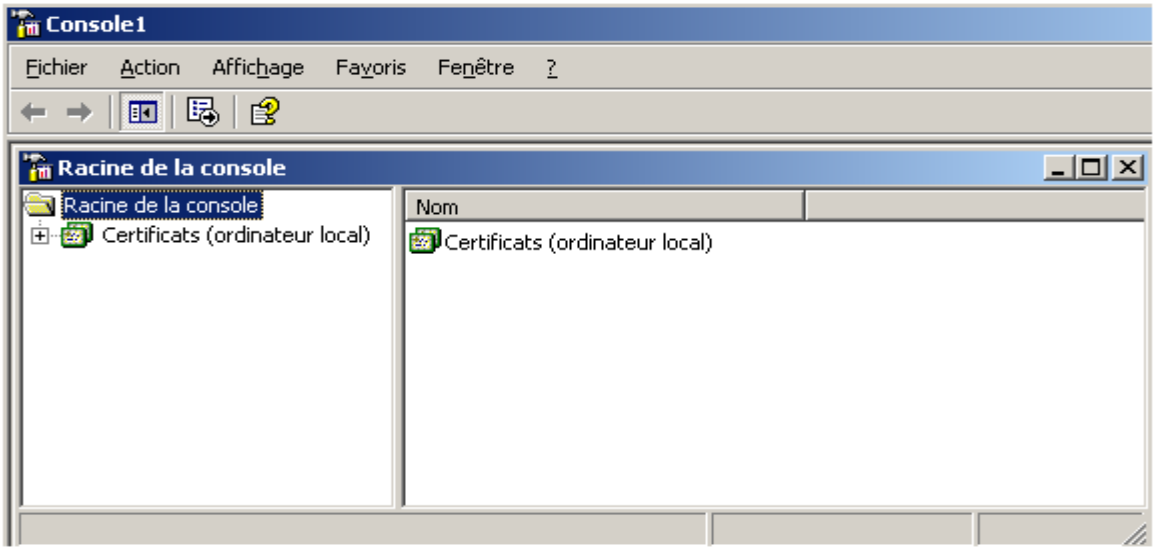
Tapez le nom du fichier, telle que celui-ci doit comporter l'extension .pfx. Par défaut, le fichier est enregistré dans le dossier Mes Documents s'il existe. Si le dossier Mes Documents n'existe pas, le fichier est enregistré dans le dossier Windows.



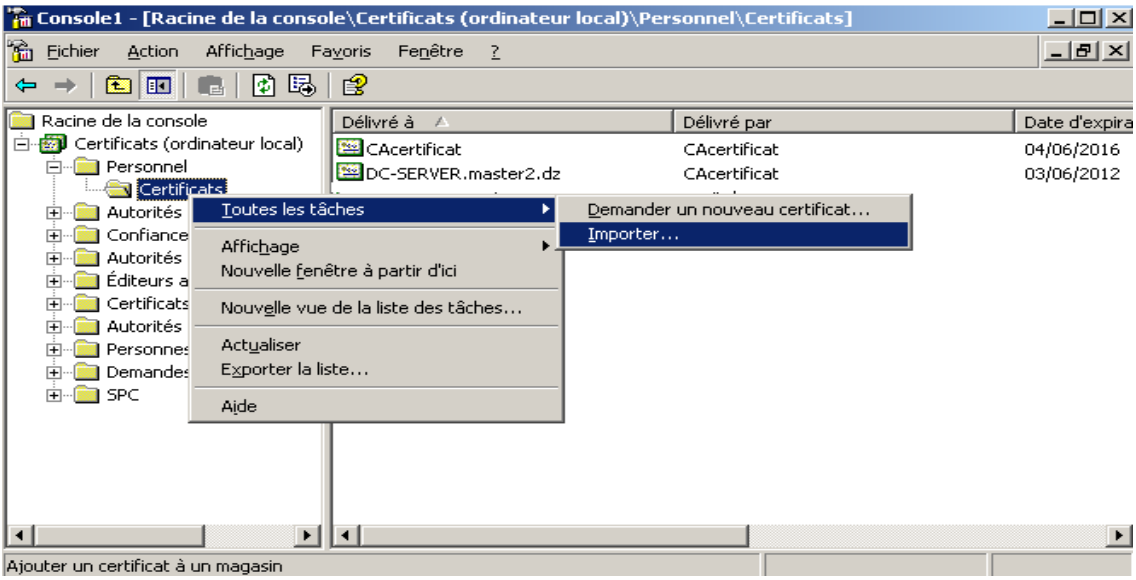
Ok pour terminer l'assistant d'Exportation de certificat.

i.2 Installation du certificat X509 pour le serveur RADIUS:

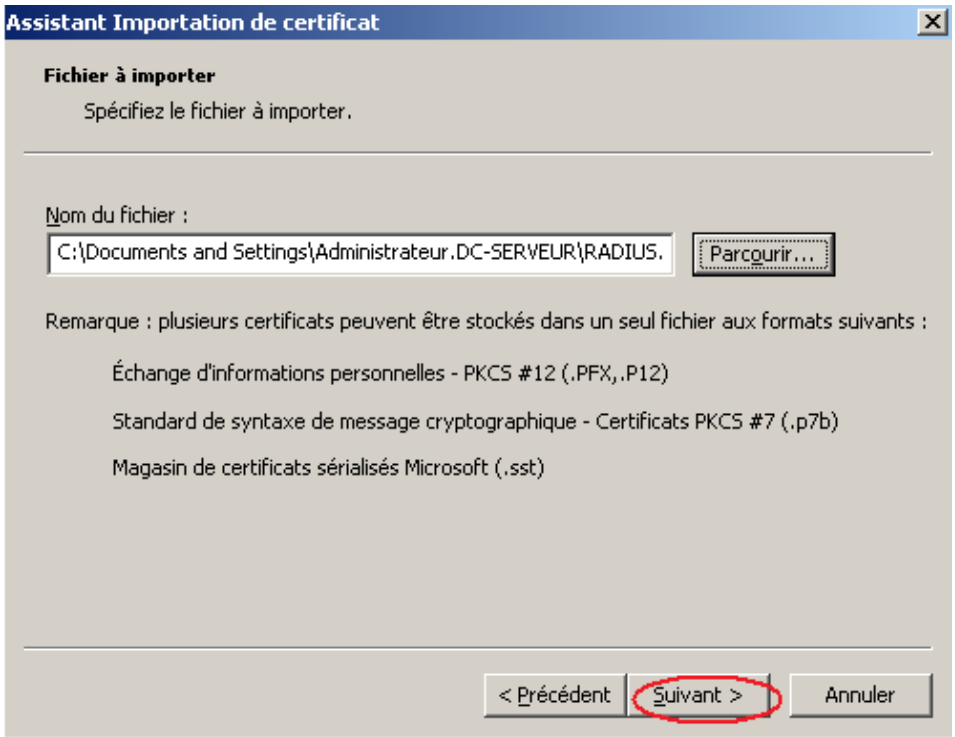
On exécute la console mmc.exe, dans le menu fichier on sélectionne Ajouter ou Supprimer un fichier enfichable, on clique sur Ajouter puis Certificats on valide par terminer :



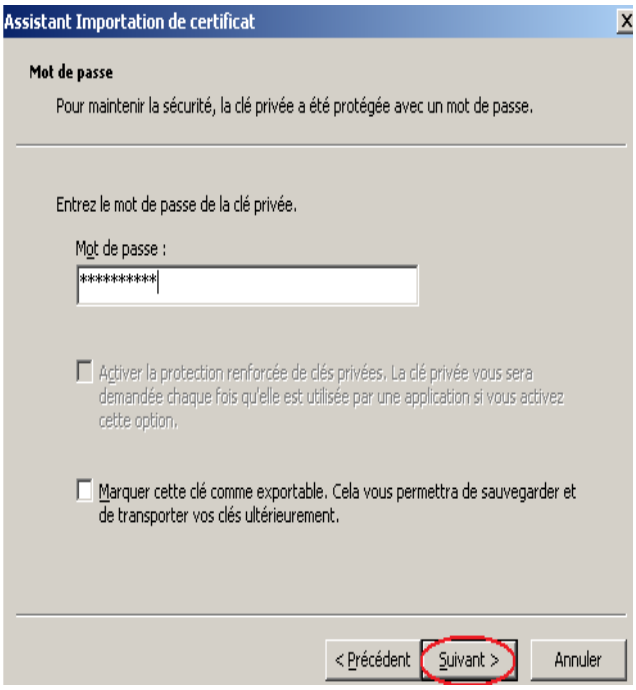
On déploie Certificats (ordinateur local)/ personnels/ certificats :

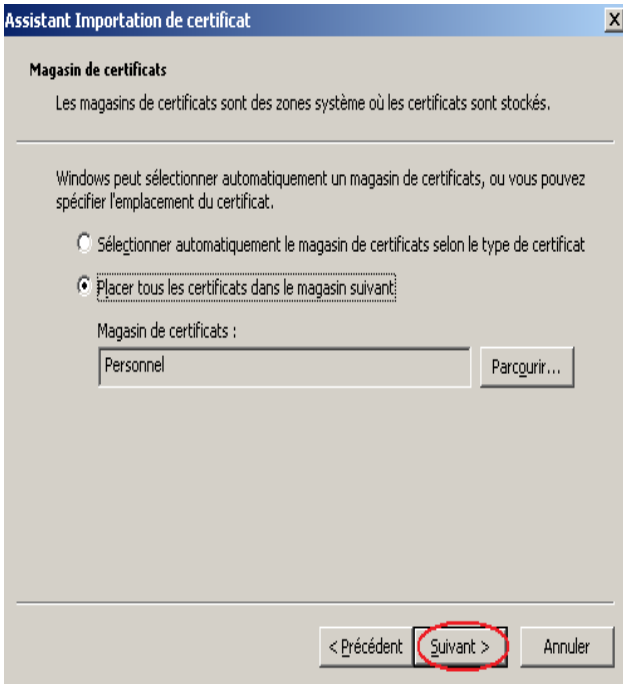


Dans la zone Fichier de certificat à importer, tapez le nom du fichier du certificat à importer, puis cliquez sur suivant.



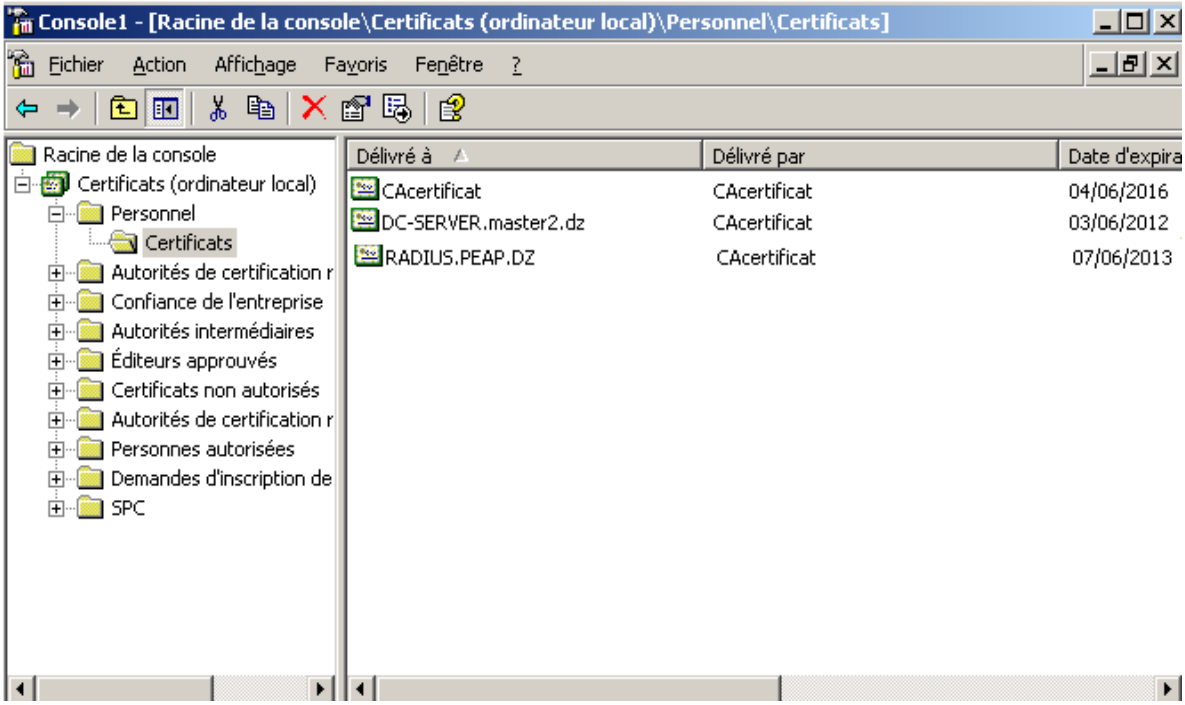
Dans la zone de mot passe, on tape le mot de passe et on place tous les certificats dans la zone Personnel.





On confirme l'importation de certificat par OK :

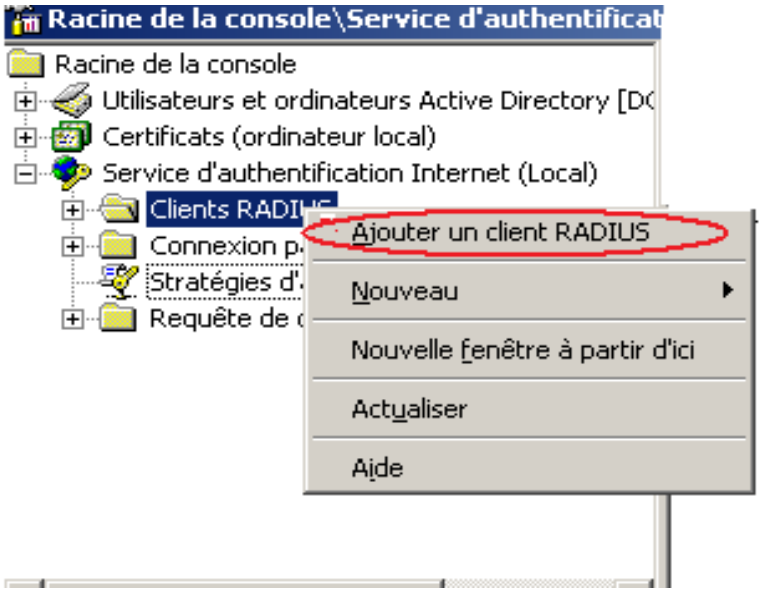
Le certificat pour l'IAS est désormais configuré avec le certificat **X509**



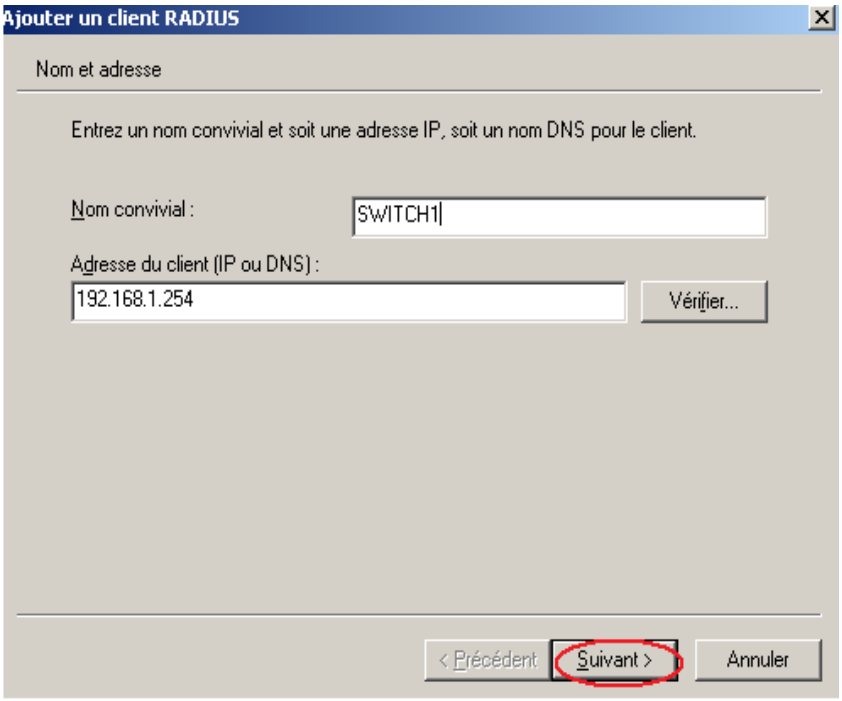
V.4.1.3.b Configuration du serveur RADIUS IAS :

i. Ajout des Clients RADIUS :

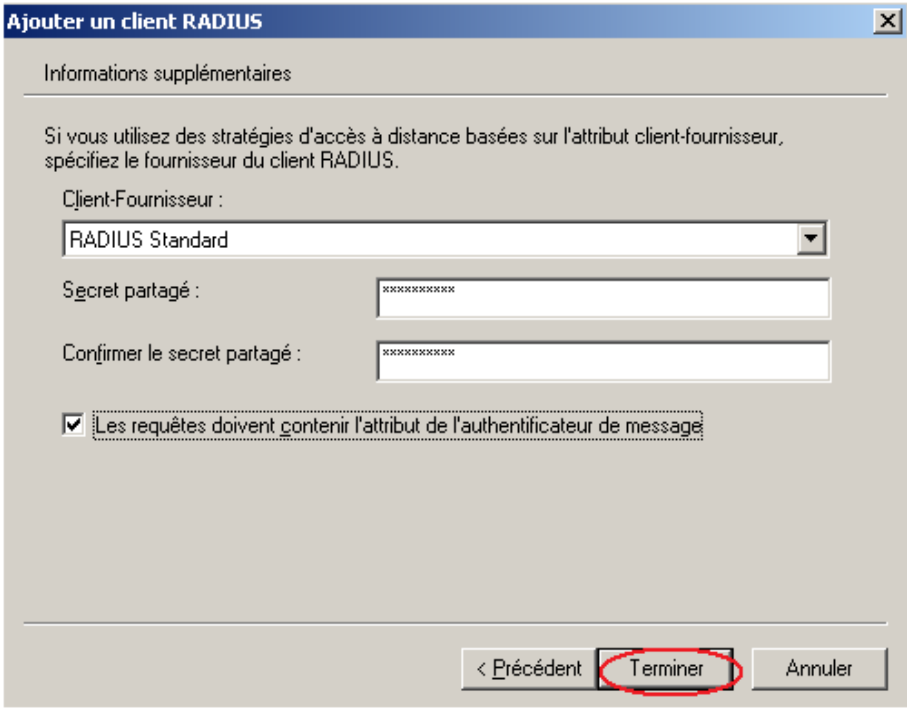
Le conteneur Clients RADIUS l'ensemble des serveurs d'accès distants qui sont des clients vis-à-vis du serveur IAS. Pour qu'un serveur d'accès distant fasse partie de cette liste, il suffit de l'y ajouter en utilisant l'assistant Ajouter un client RADIUS.



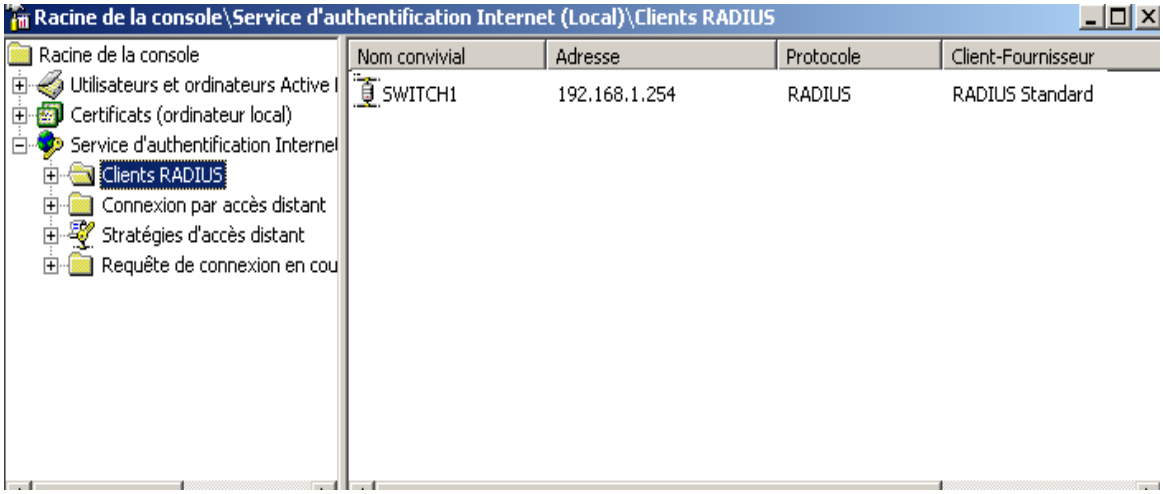
Les équipements réseaux (Switch, Serveur…) doivent être ajoutés en tant que client RADIUS. Pour qu'ils soient reconnus au niveau de serveur RADIUS. Donc pour ajouter un client RADIUS, il suffit d'entrer son nom de domaine DNS ou bien son adresse IP (dans notre cas IP : 192.168.1.254) ainsi qu'une chaîne de caractère permettant de le reconnaître facilement (exemple : SWITCH1).



Il faut ensuite choisir le type de technologie RADIUS à utiliser (ici RADIUS standard), une clé partagée (optionnelle) pour crypter et décrypter les échanges entre le client RADIUS et le serveur IAS. On peut aussi côcher la case « **Les requêtes doivent contenir l'attribut de l'authentificateur de message** » qui aura pour effet de forcer le client RADIUS à s'authentifier à chaque connexion auprès du serveur IAS en envoyant une signature numérique.



- On clique sur terminé la fenêtre suivante apparait :



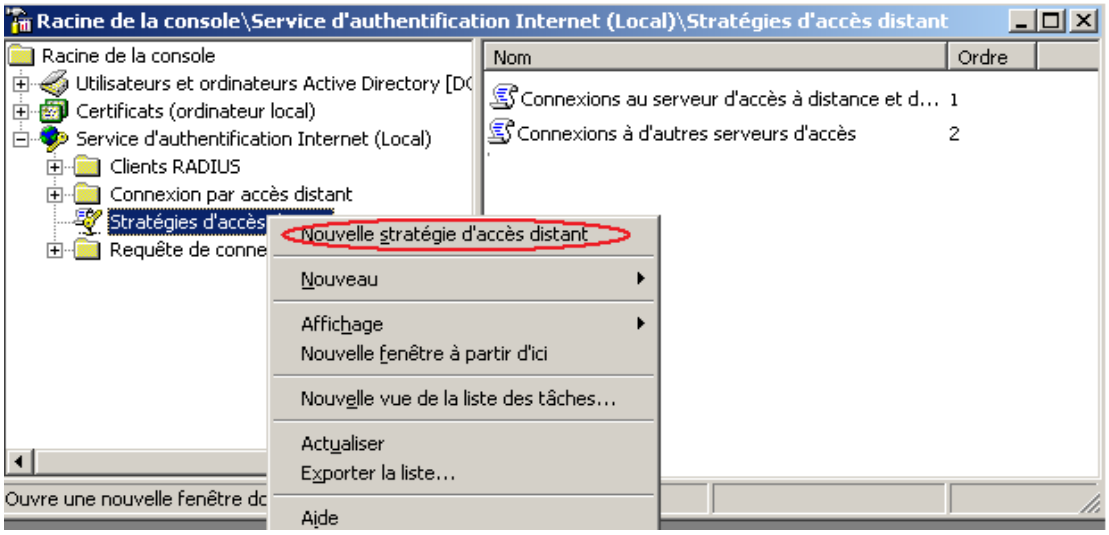
Cette manipulation est à répéter pour chaque équipement réseau qui aura l'authentification **802.1x** à activer.

ii. Stratégie d'accès distant :

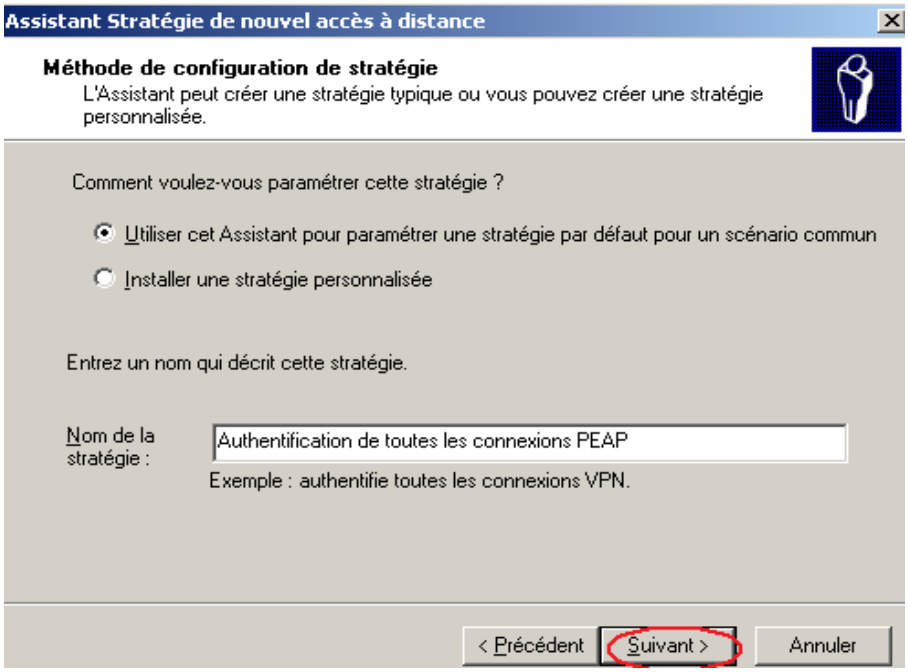
Une stratégie d'accès distant est un ensemble de conditions définissant qui pourra accéder à distance au réseau et quelles seront les caractéristiques de cette connexion. Les critères d'acceptation ou de refus de connexions sont très variés. Il est possible de configurer une stratégie pour refuser ou accepter une connexion suivant une plage horaire, appartenance à un groupe, type de service, protocole utilisé, temps maximum de connexion etc… L'ordre de placement des stratégies est très important car c'est la première stratégie concernée qui servira à accepter ou refuser la connexion.

- La stratégie d'accès distant par défaut de l'IAS rejette tout client qui essaie de se connecter, même s'il est authentifie. Une nouvelle stratégie doit être mise en place pour accorder l'accès aux clients qui s'authentifient correctement.

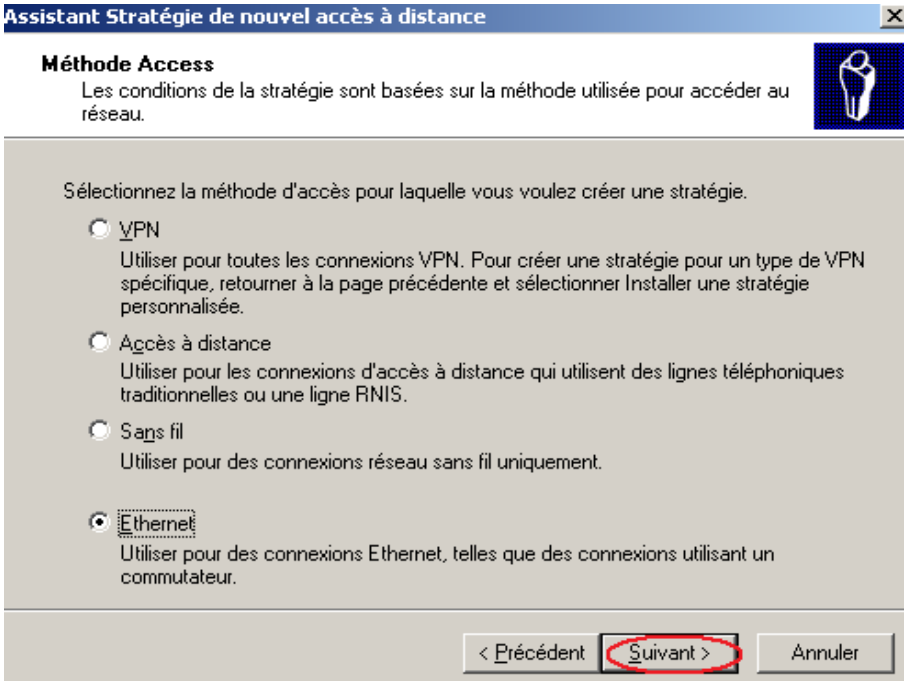
Tout d'abord allez dans le menu Démarrer puis Outils d'administration et enfin sélectionnez Service d'authentification Internet. Dans le dossier Stratégie d'accès distant faites un click droit puis nouvelle stratégie d'accès distant.



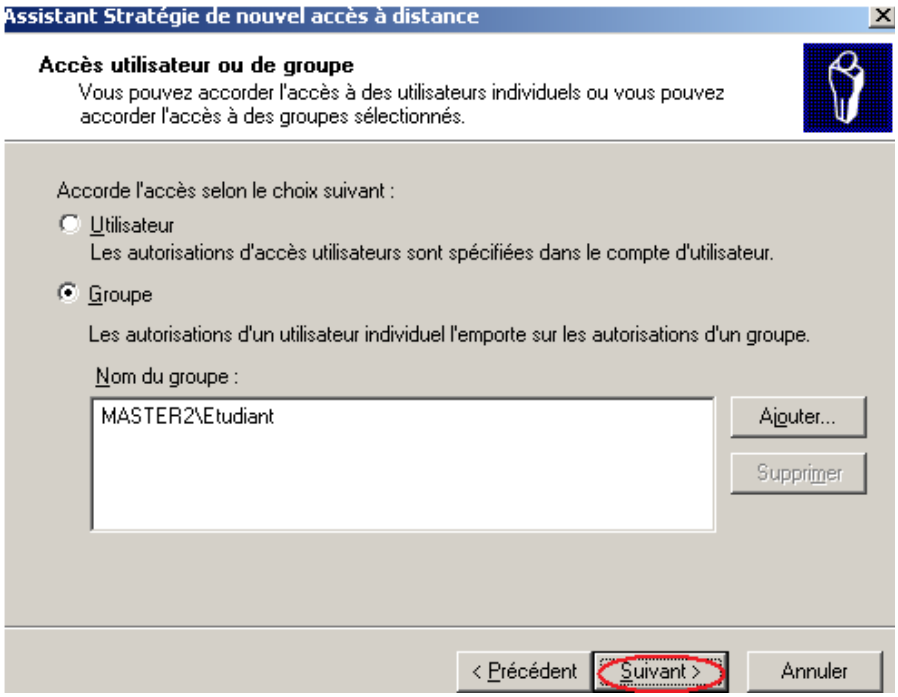
- Cochez utiliser cet assistant pour paramétrer une stratégie par défaut pour un scénario commun. Puis entrez le nom de la nouvelle stratégie.



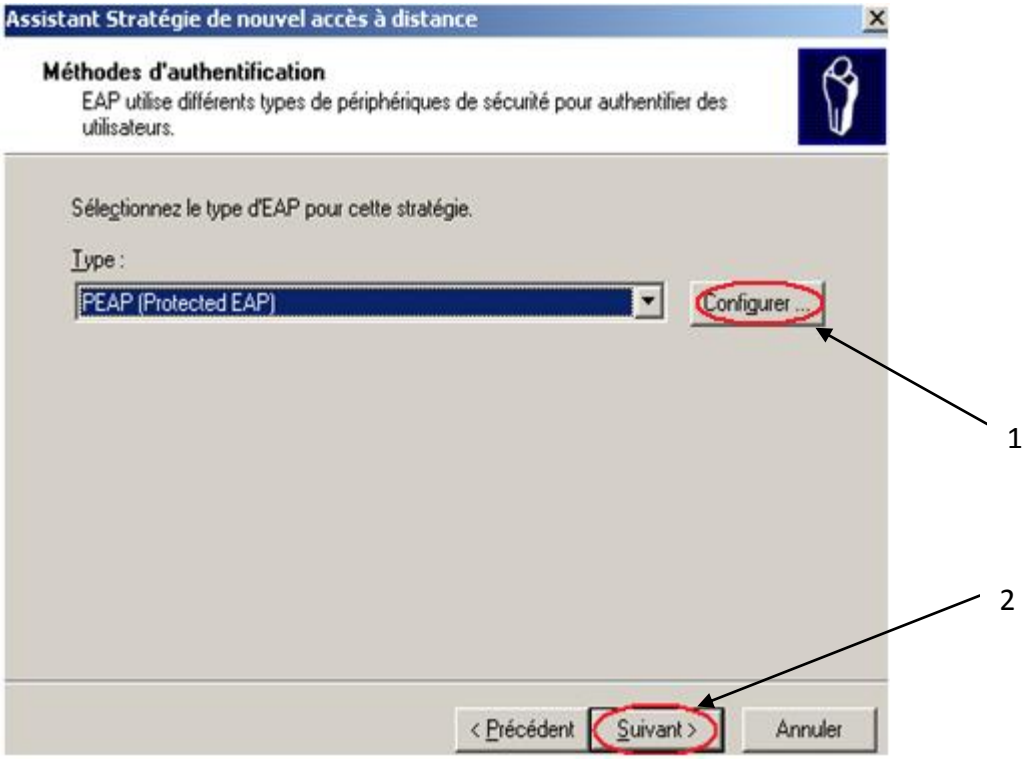
La fenêtre ci-dessus montre les différentes méthodes utilisées pour accéder au réseau, dans notre cas on sélectionne **Ethernet** car il s'agit d'une connexion via un Switch.

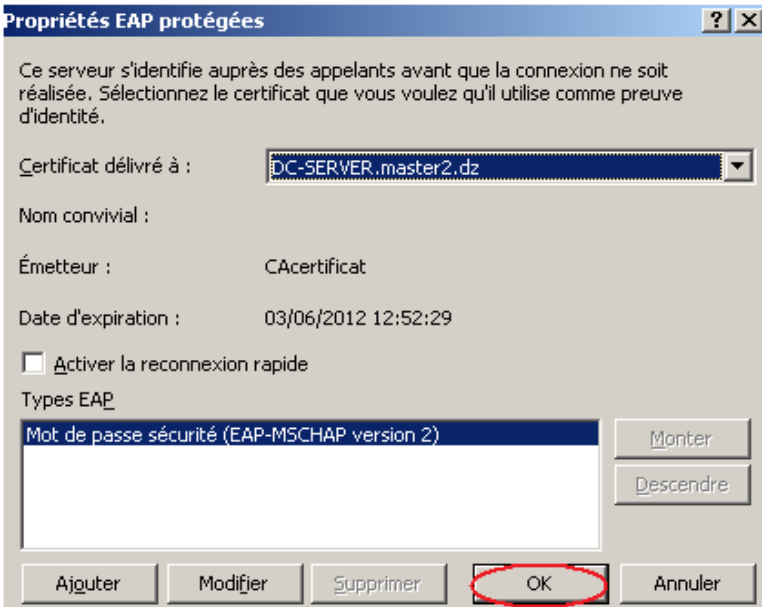


Dans la boite de dialogue suivante, on doit spécifier à quel groupe à qui l'utilisateur doit appartenir pour pouvoir accéder par l'intermédiaire de cette stratégie, on sélectionne alors le groupe et on clique sur suivant.



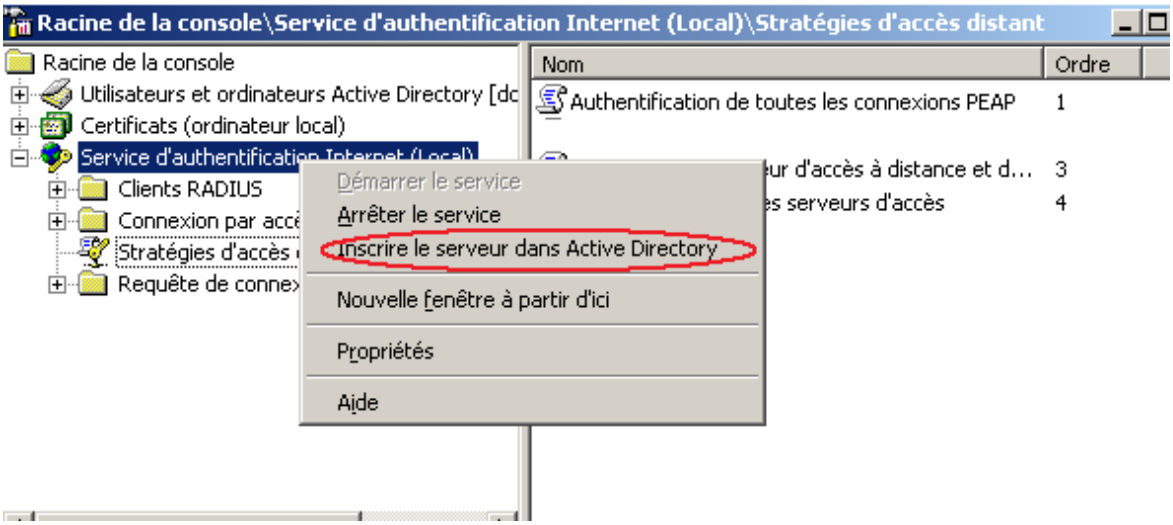
Ensuite, on choisit la méthode d'authentification (PEAP (Protected EAP)) et on clique sur configurer pour vérifier que le certificat est délivré au serveur à DC-SERVER.master2.DZ (nom DNS du serveur) par l'autorité de certificat.





V.4.1.3.c Enregistrement du serveur IAS :

Une fois le serveur RADIUS « IAS » est configuré il faut l'enregistrer dans le domaine Active Directory pour qu'il puisse communiquer. Pour ce faire aller dans le gestionnaire ''Service d'Authentification Internet '' et faites clique droit sur celui-ci et ensuite clique sur ''inscrire le serveur dans Active Directory''.



Le serveur IAS est maintenant prêt à accepter des messages RADIUS provenant du Switch.

V.2 Configuration du supplicant :

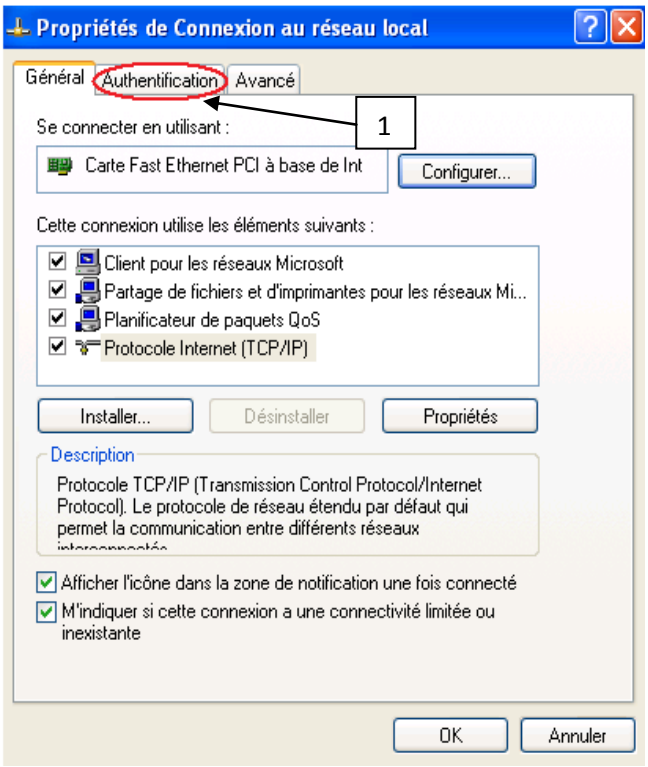
Les postes clients (supplicants) doivent être configurés pour qu'ils puissent connecter au Switch à travers un port utilisant l'authentification **802.1x**. Il est nécessaire que le poste client supporte le protocole.

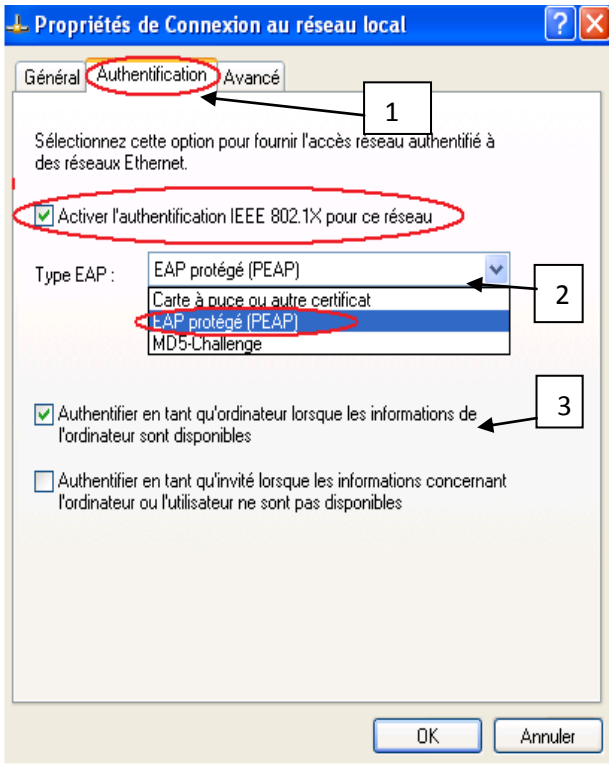
V.2.1Activation de 802.1x et choix de la méthode utilisée :

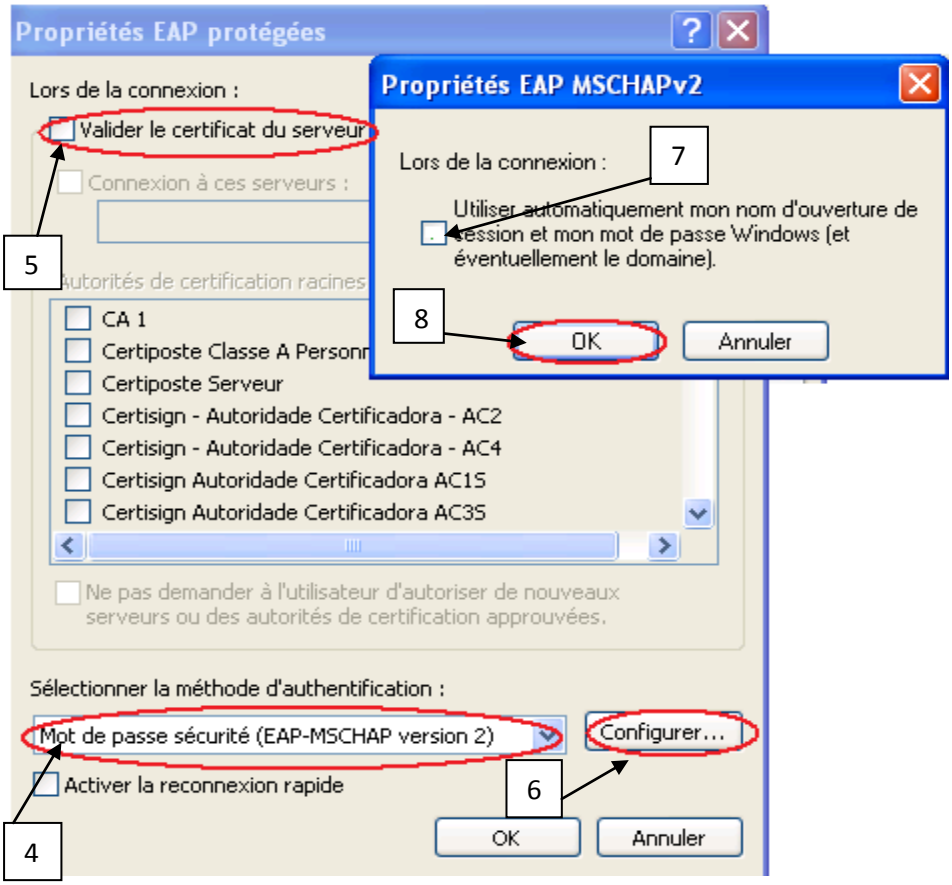
Pour ce faire, il suffit d'accéder au panneau de configuration de la connexion réseau souhaité, puis sélectionner l'onglet « Authentification ». On active l'authentification IEEE 802.1x pour ce réseau et on sélectionne la méthode EAP protégé (PEAP), puis on clique sur propriété un choix nous est proposé, on décoche la case « Valider le certificat du serveur » qui permet de configurer ce client de telle sorte qu'il ne se connecte au réseau que si le certificat de serveur est validé et on choisit la méthode d'authentification « mot de passe sécurisé (EAP-MSCHAP version2) ».

On clique sur configurer la boite de dialogue « propriétés EAP MSCHAPv2 » s'affiche, si la case de celle-ci est cochée la station de travail se connecte au réseau avec les paramètres d'identification de l'utilisateur enregistré. Dans le cas contraire, quand un autre utilisateur essaie de se connecter au réseau à travers la même station, un message lui demandant de s'authentifier s'affiche.

V.2.2 Illustration de la configuration de Client 802.1x :







V.3 Configuration de L'authentificateur (Switch Cisco) :

Le Switch utilisé pour cette configuration est de type Cisco catalyst 2950 et 2960 qui supporte l'authentification avec l'annuaire RADIUS.

V.3.1 Activation de 802.1x sur le port du Switch Cisco:

L'état de port d'un Switch est configuré à l'aide de la commande suivante :

Switch (config-if) #dot1x port-control : Cette commande peut être utilisé en trois fonctions :

Force-authorized : Aucune authentification n'est exigée et le port laisse passer tout le trafic.

Force unauthorized : Aucune authentification et le port bloc tout le trafic.

Auto : Authentification **802.1x** activée, si le client est authentifié correctement le port permettra d'accéder aux ressources de réseau demandées par le client jusqu'à ce qu'il se déconnecte.

Dans notre cas on exécute la commande suivante :

Switch (config-if) #dot1x port-control auto (Activation de l'authentification 802.1x)

Par défaut les ports de Switch sont en mode dynamique afin de lui permettre de négocier avec l'interface voisine si le port doit devenir TRUNK ou non.

802.1x ne peut pas être appliqué sur n'importe quel port. Il faut donc désactiver le mode dynamique à l'aide de la commande : **Switch (config-if) # Switchport mode access.**

V.3.2 Les différentes commandes utilisées pour configurer un Switch Cisco :

Pour configurer un Switch Cisco on applique les commandes suivantes :

Switch (config) # aaa new-model: Activation de l'authentification
Switch (config)# aaa authentication dot1x default group radius
Switch (config)# dot1x system-auth-control
Switch (config) # interface fastEthernet 0/1
Switch (config-if) #Switchport mode vlan 2
Switch (config-if) #Switchport mode access: désactivation du mode dynamique.
Duplex full
Speed auto
Switch (config-if) # dot1x port-control auto : Activation de 802.1x sur le port.
Interface vlan2
IP adresse xxxxxxxxxxx 255.255.255.0

La commande ci-dessous permet de déclarer le serveur RADIUS dans le Switch en spécifiant l'adresse IP de serveur, elle permet aussi de définir le secret partagé entre les deux équipements.

Switch (config) # radius-server host xxxxxxxx key xxxxxxx

V.3.2 Simulation d'un Switch Cisco a l'aide d'un émulateur GNS3 :

Le but de cette partie est de présenter comment configurer l'authentification **802.1x** au niveau d'un Switch Cisco en vue de sécuriser l'accès physique au réseau local, pour commencer on présente le simulateur réseau GNS3 (Graphical Network Similator 3).

- **Généralités sur le simulateur « GNS3 »:**
- **Définition :**

GNS3 est un simulateur graphique d'équipements réseaux qui nous permet de créer des topologies de réseaux complexes et d'en établir des simulations. Ce logiciel, en lien avec Dynamips (simulateur IOS (Internetwork Operating System)), Dynagen (interface textuelle pour Dynamips), est un excellent outil pour l'administration des réseaux CISCO, les laboratoires réseaux ou les personnes désirant s'entraîner avant de passer les certifications **CCNA, CCNP, CCIP ou CCIE.** De plus, il est possible de s'en servir pour tester les fonctionnalités des IOS Cisco ou de tester les configurations devant être déployées dans le futur sur des routeurs réels.

GNS3 fonctionne sous les systèmes d'exploitation suivants : WIN 98, XP, WIN7.Linux

Le gros avantage de **GNS3** est qu'il évite de dépenser beaucoup d'argent dans des équipements CISCO qui coûtent très chers, et de pouvoir manipuler et tester, comme dans un environnement réel.

- **Technologie et protocoles supportés :**

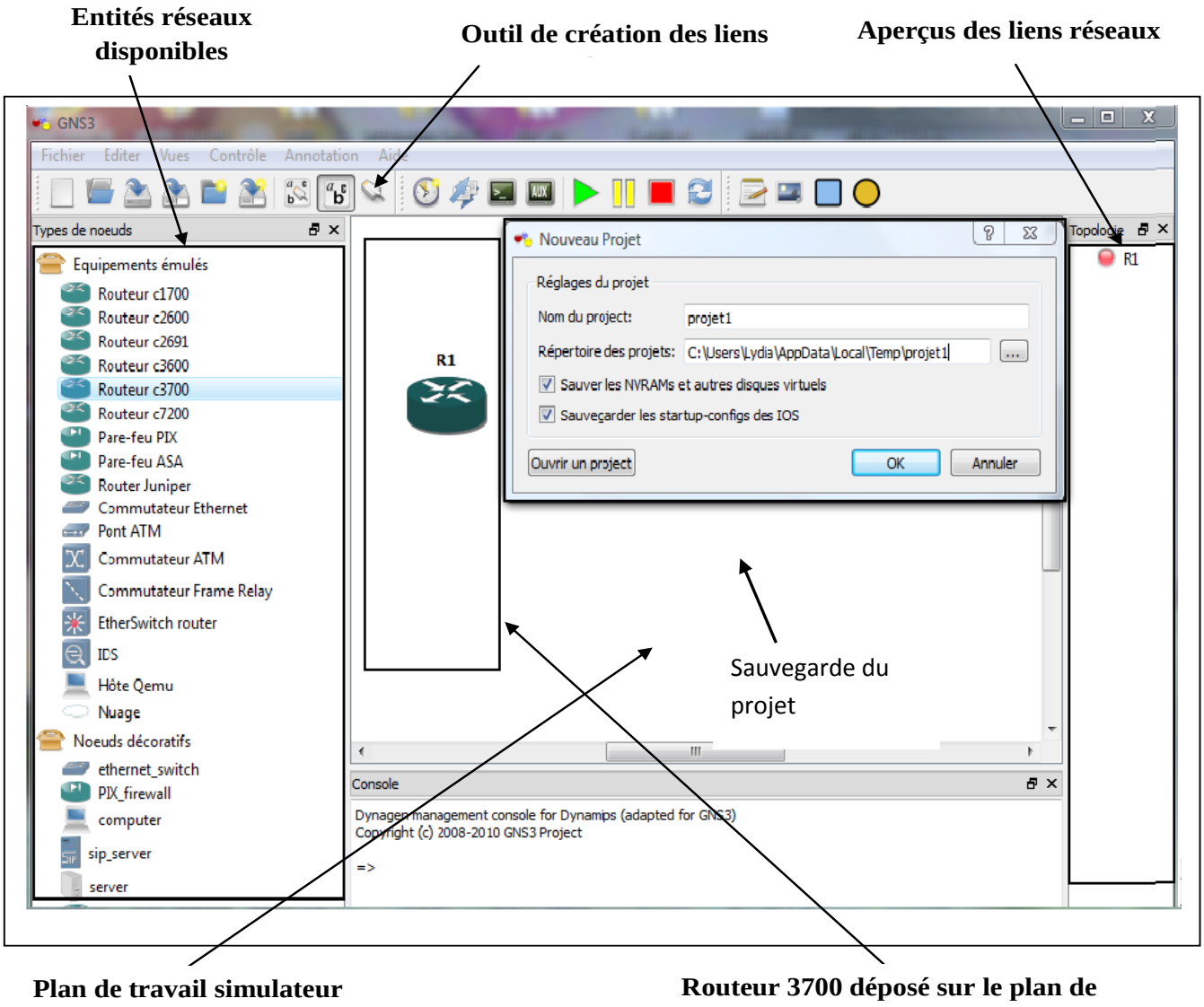
GNS3 supporte toutes sorte de câbles (FastEthernet, Gigabit Ethernet, Câble série, Fibre optique) ainsi que les technologies suivantes : VLAN, VLSM, DHCP, comme il introduit les couches du modèle OSI lors de l'acheminement du paquet.

Il supporte les équipements suivants : Routeur (3700, 2600,3600, 1700, 7200, PIX, ASA…).

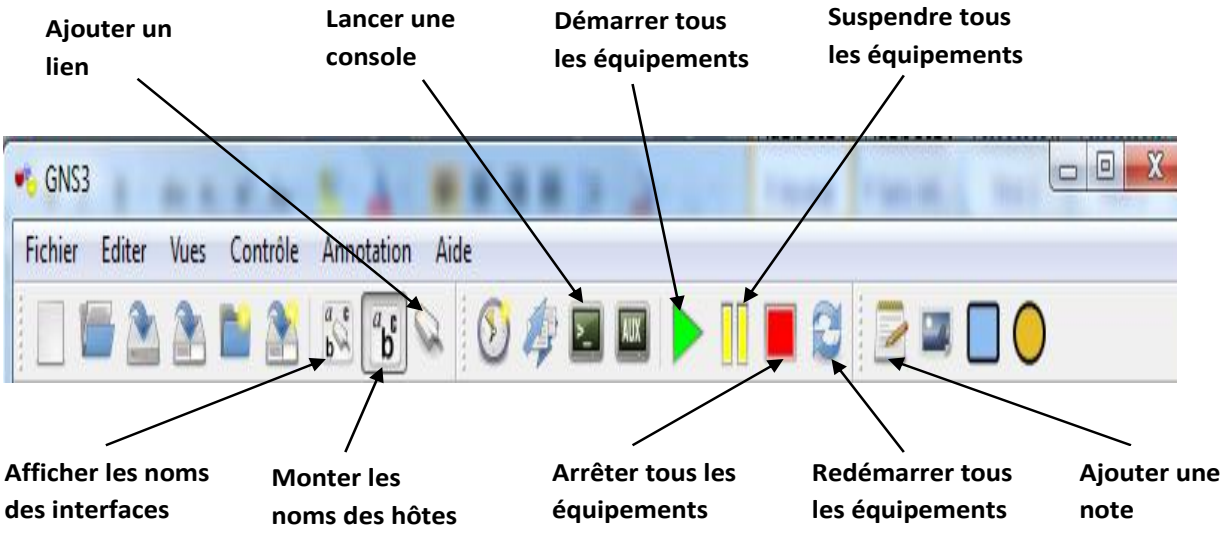
Cet outil permet de simuler le hardware de Cisco et utilise les vrais IOS Cisco. Il est donc indispensable d'avoir accès à l'IOS de Cisco.

Quand on œuvre le simulateur **GNS3** la fenêtre suivante s'affiche :

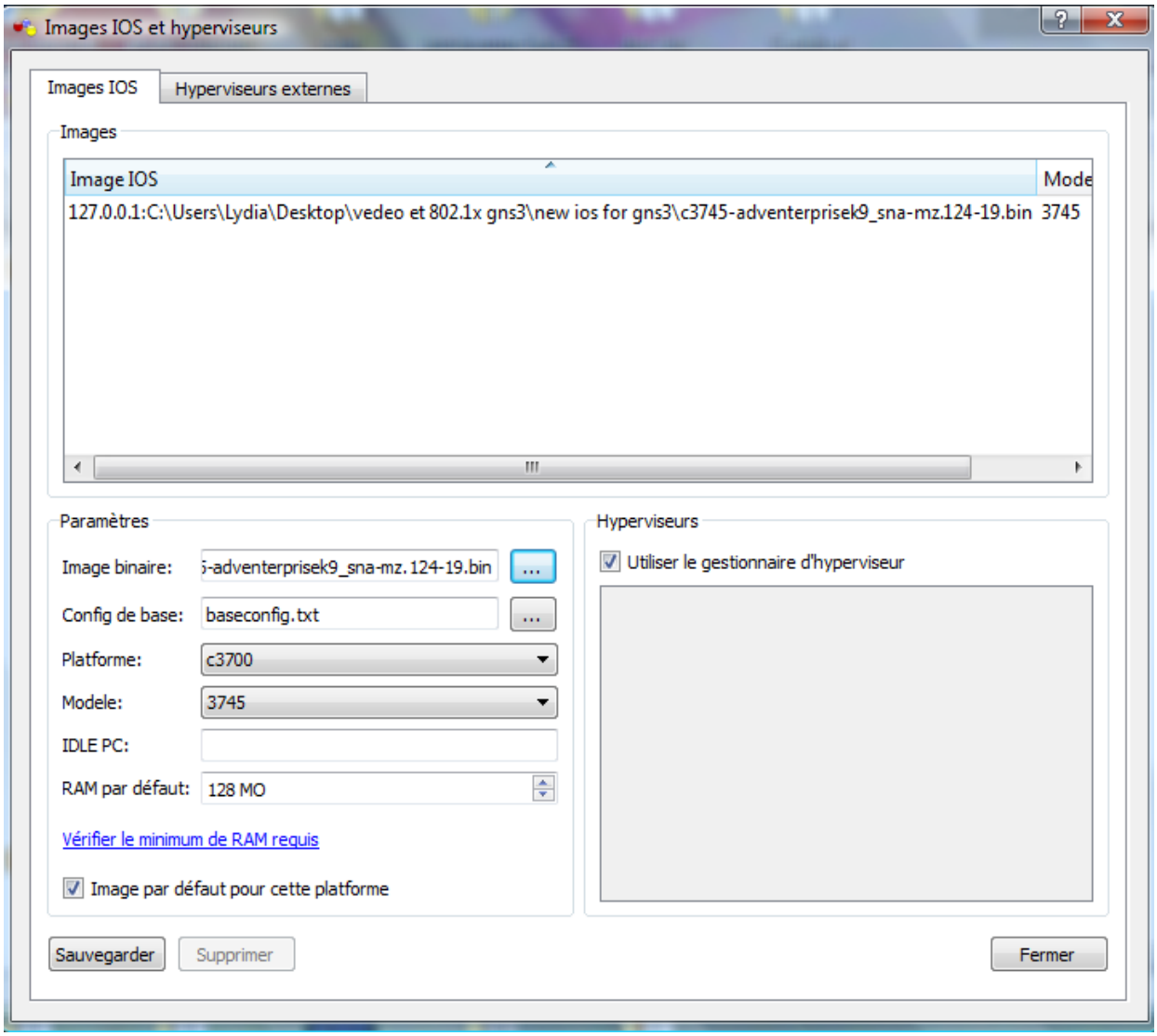
❖ **Détails de la fenêtre simulateur :**



❖ **Les éléments de la barre outils de GNS3 :**

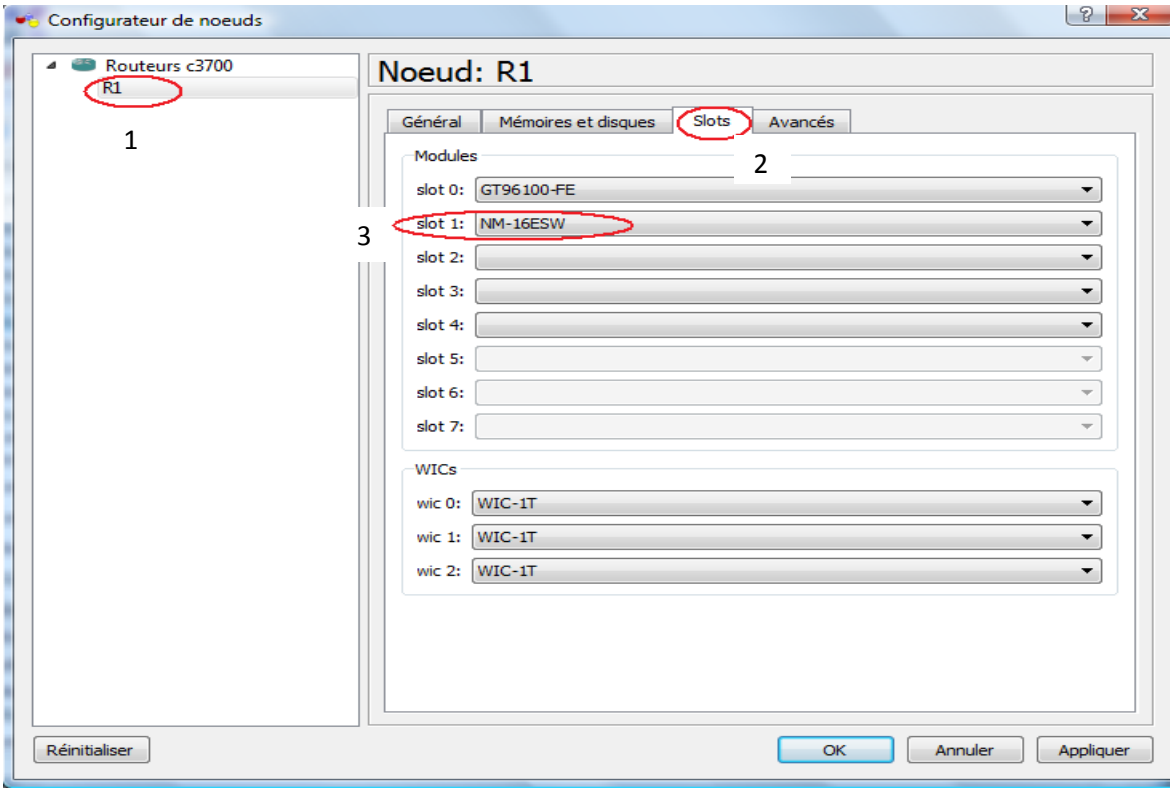


- **Ajout d'un IOS Cisco à GNS3 :** Dans GNS3, cliquez sur Éditer, puis Images IOS et hyperviseurs. Une fenêtre vous permettant d'ajouter des IOS s'ouvre.

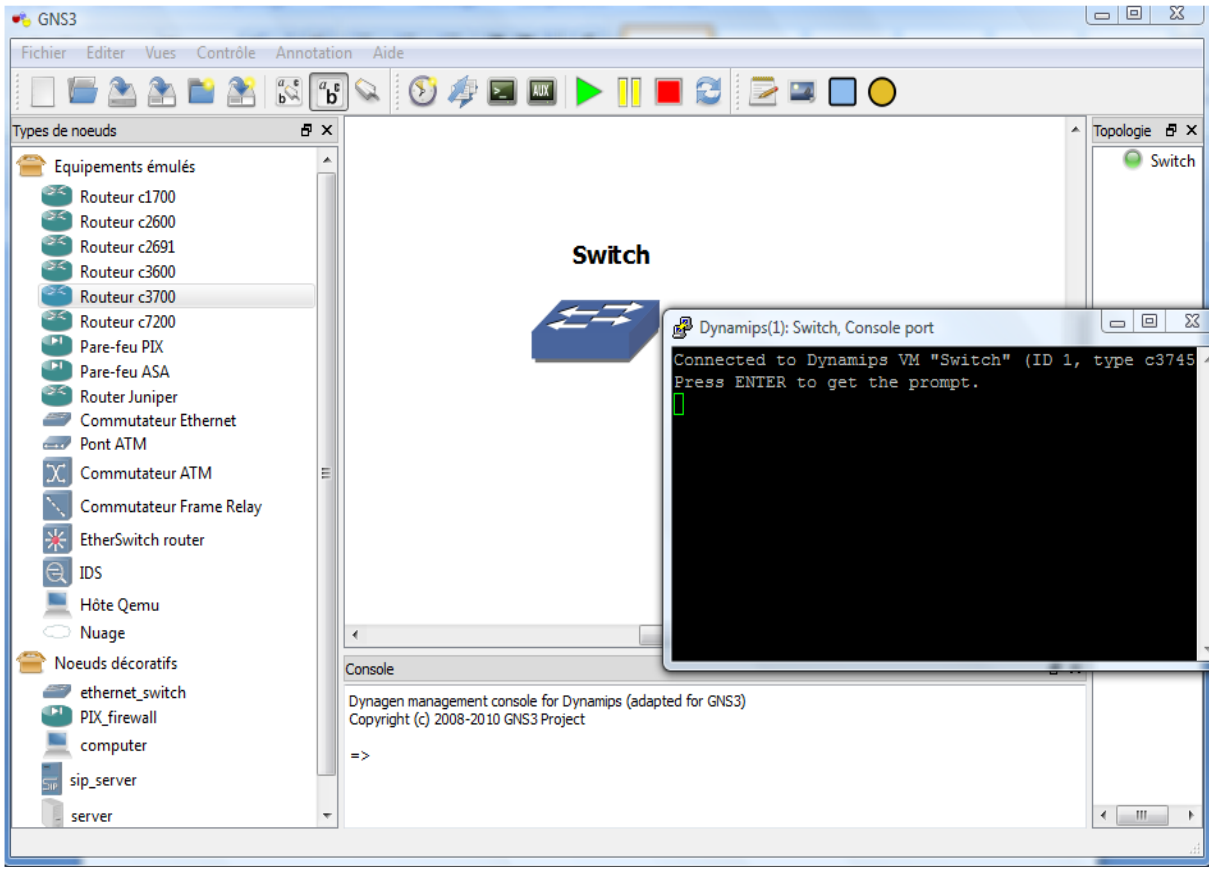


L'émulation des Switch Cisco catalyst dont on a besoin pour notre configuration n'est pas supporté par le simulateur GNS3 car l'architecture des circuits ASIC de leurs processus est complexe pour reproduire dans ce simulateur. Mais un module de Switching Ethernet (référence Cisco NM-16ESW) peut être utilisé sur les plateformes 3700, 3600,2600. En ajoutant ce module, le retour va acquérir les fonctionnalités d'un Switch.

Afin d'utiliser le routeur que nous avons sélectionné précédemment comme Switch, il suffit de le sélectionner dans le menu de droite (configurateur de nœuds**),** sélectionne l'icône ''Slots '' et on choisit la référence Cisco NM-16ESW.

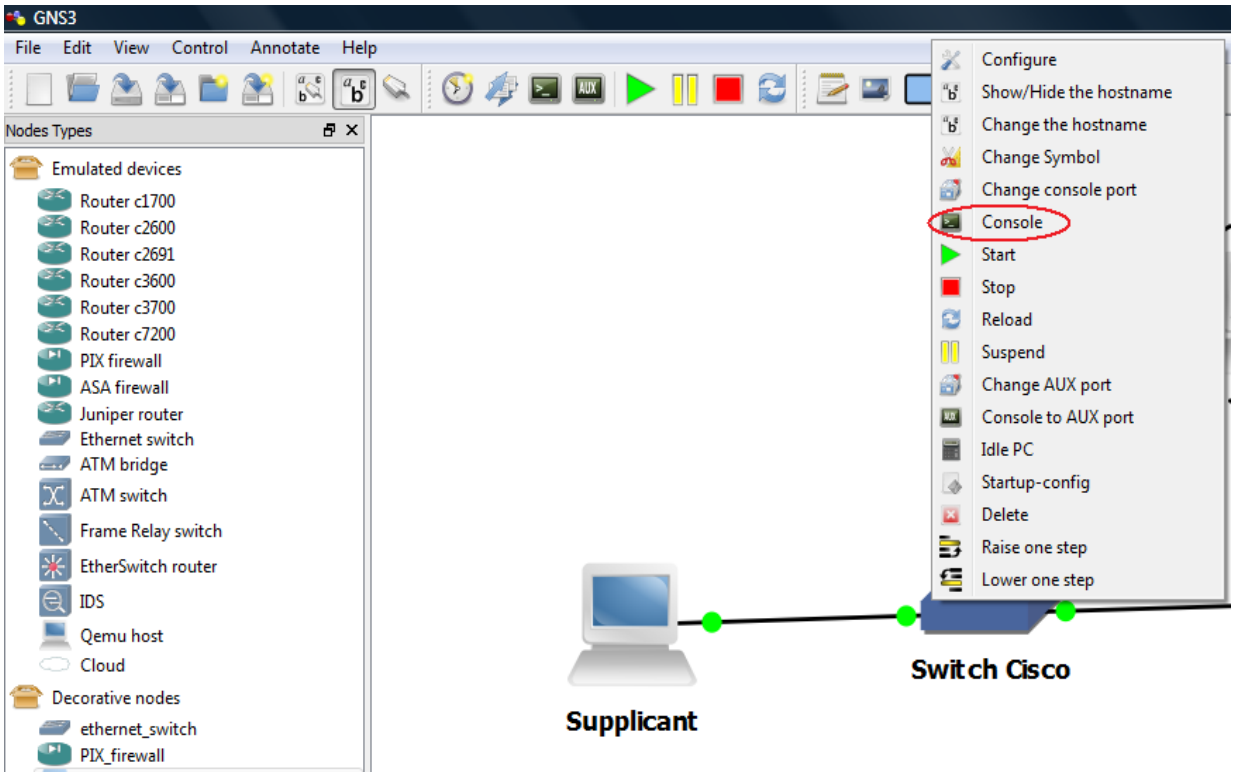


Il ne reste à présent plus qu'à démarrer le Switch. Cliquez-droit sur le celui-ci puis Démarrer. Dans le cadre topologie, on observe alors que le voyant relatif au Switch est à présent vert. Pour accéder à la console d'administration du Switch cliquez-droit sur le Switch puis cliquez sur "Console". L'interface console du Switch s'ouvre alors.

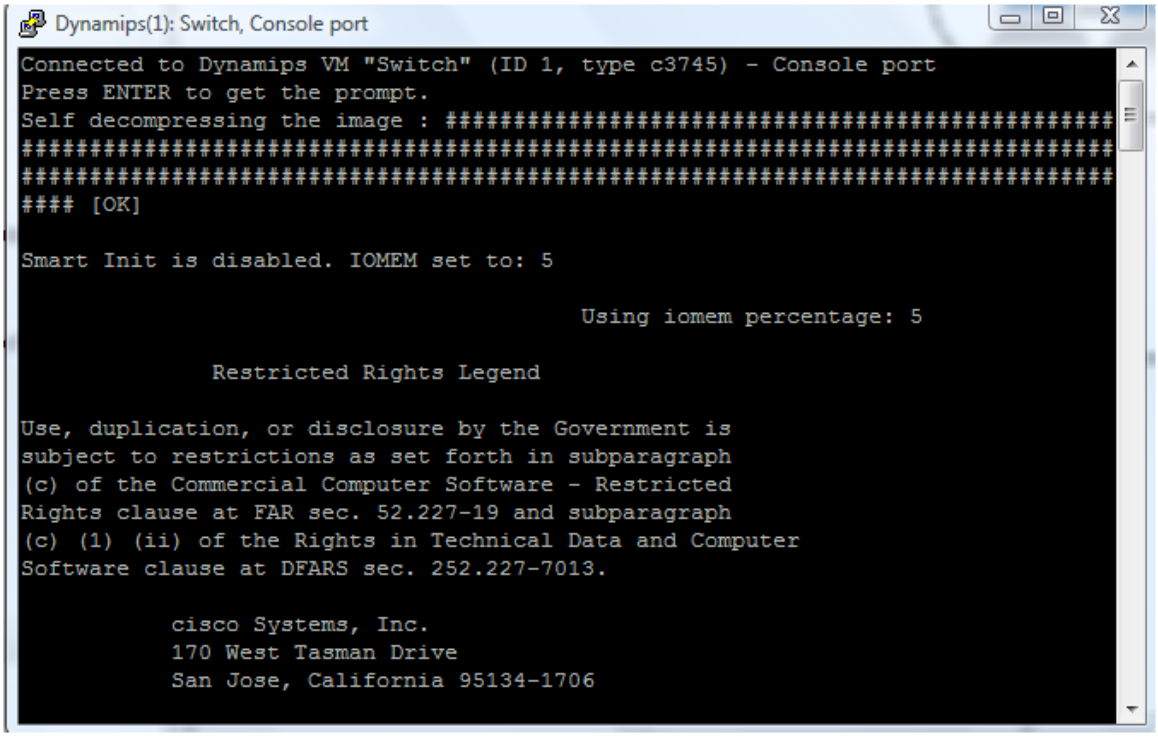


Une fois la topologie de notre réseau est réalisée, on procède à la configuration de notre Switch et pour cela on suit les différentes étapes suivantes :

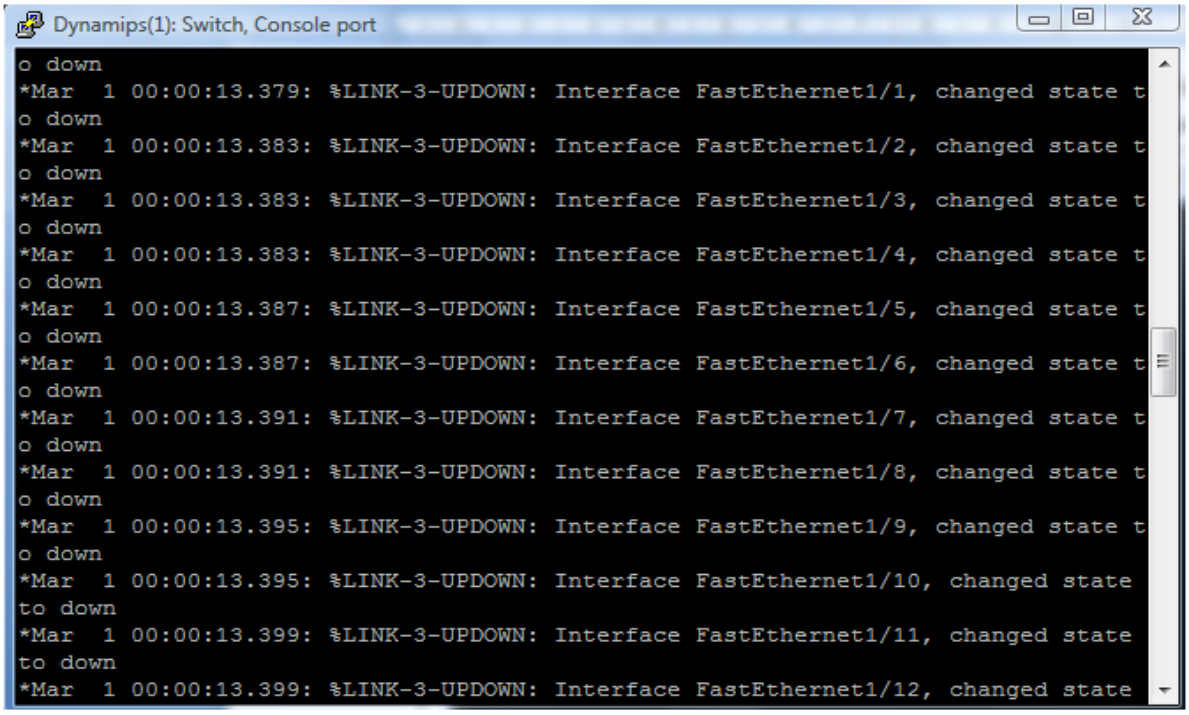
- On clique sur le bouton droit de la souris sur le Switch, la fenêtre suivante s'affiche :



- On sélectionne le mode console, le Switch procède au chargement de son système de fonctionnement (Image IOS) a partir de sa mémoire NVRAM.



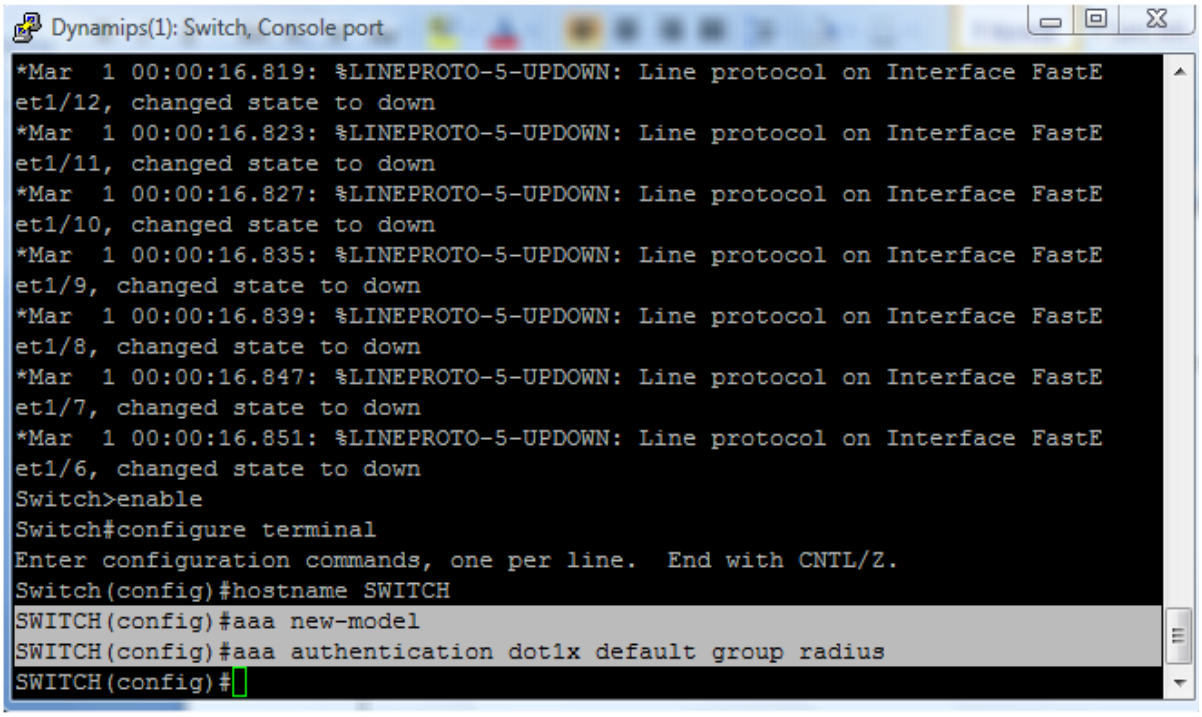
❖ Avant l'implémentation de notre configuration on vérifie que les fonctions de Switch sont bien intégrées au retour, en exécutant la commande **« Show running - config »**

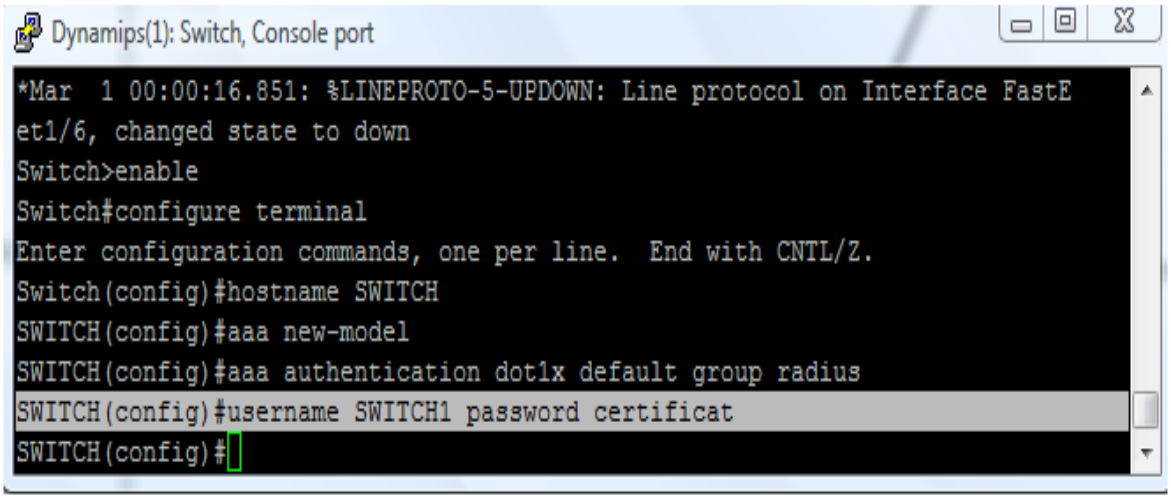


On remarque que le retour possède les propriétés de Switch.

❖ **Cette configuration a pour but d'activer l'authentification AAA et 802.1x sur le port FastEthernet .**

❖ **Implémentation du modèle aaa :**

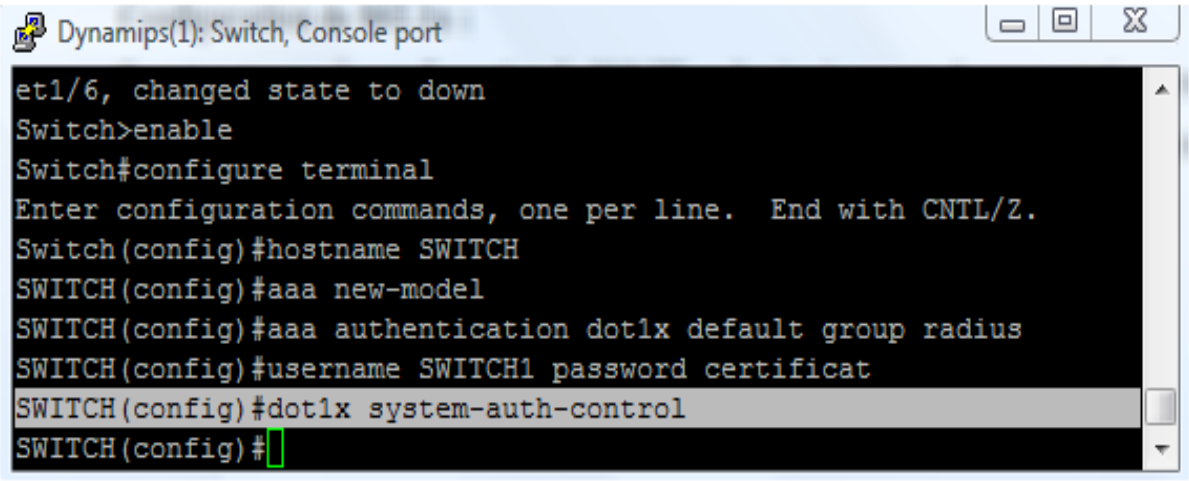




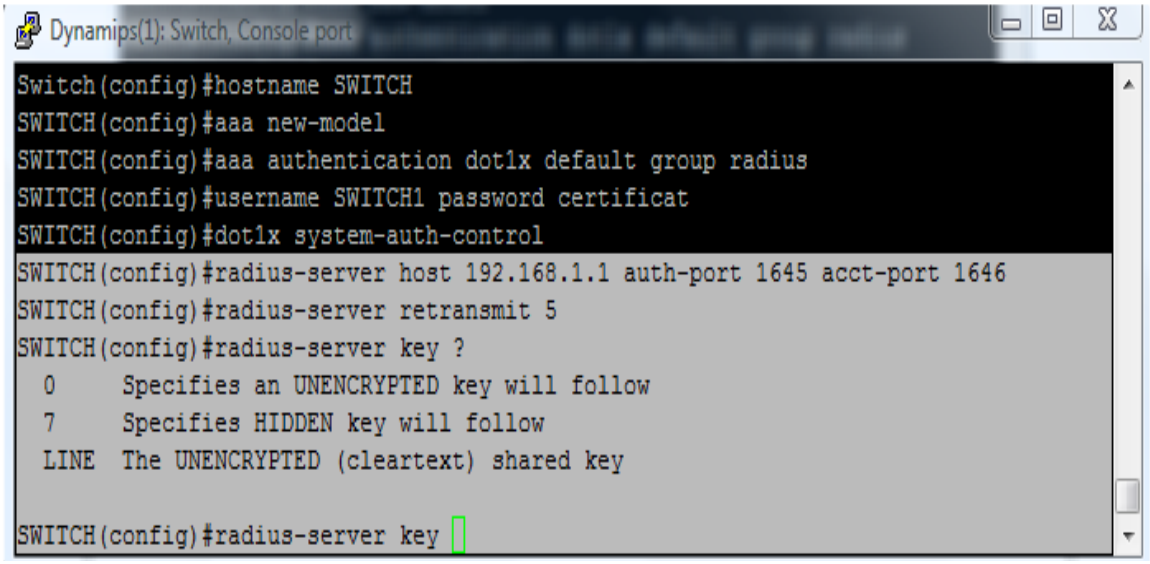
Cette dernière commande a comme rôle de permettre au Switch l'accès au serveur RADIUS via son compte (Client RADIUS) crée dans Active Directory.

- **Configuration de 802.1x :**

Il est à noter que la configuration du **802.1X** sur les équipements de commutation peut s'effectuer de façon globale. Il est alors primordial de prendre en compte les interactions entre les divers commutateurs interconnectés (paramètre « **dot1x system-auth-control** »).



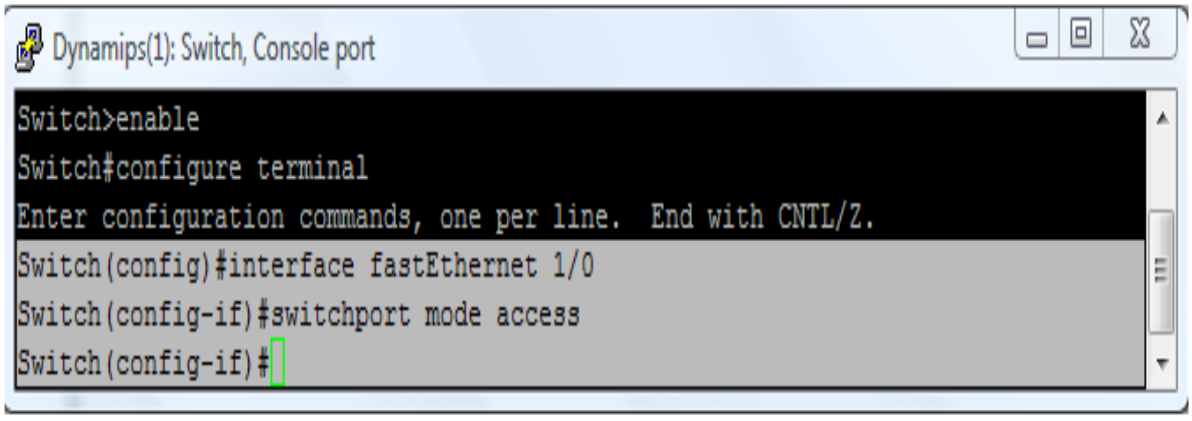
- Configuration de l'adresse IP de serveur RADIUS et de la clé secrète partagée avec le client RADIUS.



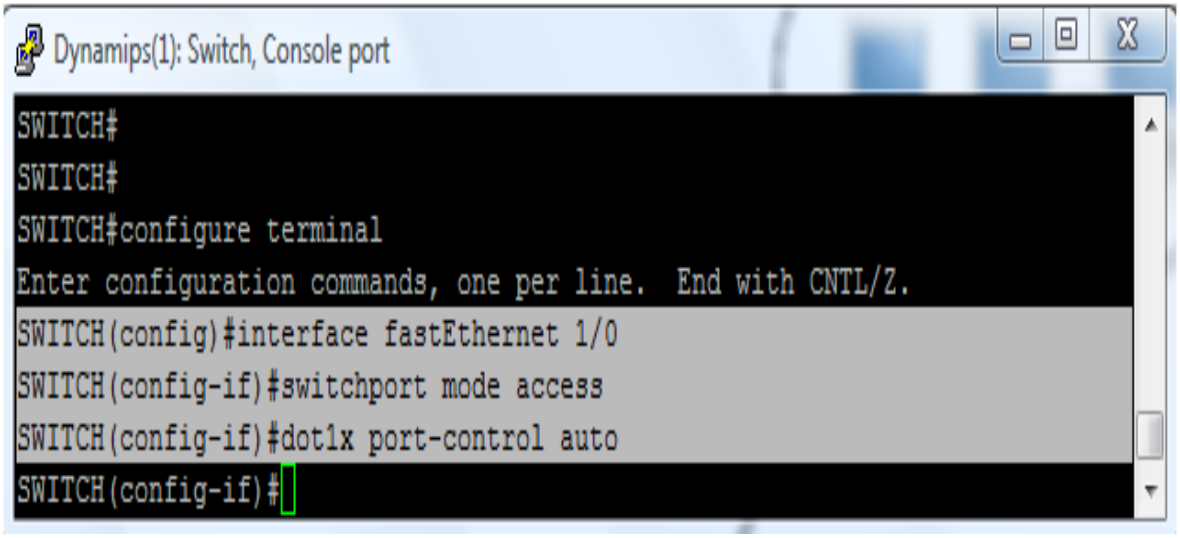
❖ **Ces différentes commandes servent à :**

- **Radius-server host 192.168.1.1 auth-port 1645 acct-port 1646** : permet de configurer les paramètres de serveur RADIUS sur le commutateur (indiqué le nom ou l'adresse IP de serveur RADIUS), qui utilise le port UDP 1645 pour l'authentification et le port 1646 pour l'Accounting, c'est à dire la gestion des informations récoltées pendant toute la durée de la session, après identification de l'utilisateur.
- **radius -server retransmit 5 :** spécifier le nombre de fois que le client essayer de s'authentifier au server avant que ce dernier lui coupe la connexion.
- **Radius server-key** : permet d'indiquer la clef de chiffrage utilisée entre le commutateur et le serveur RADIUS.

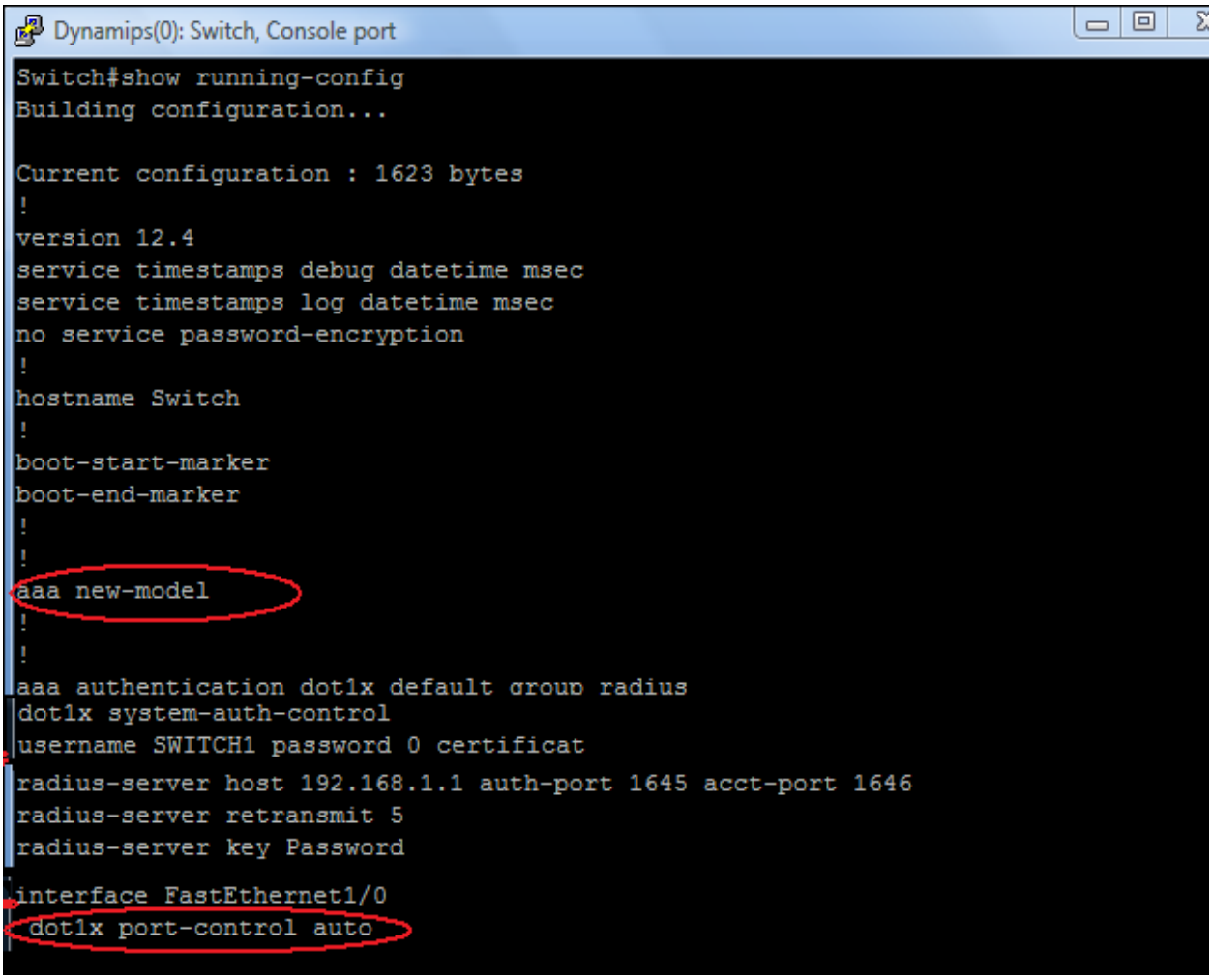
❖ **Configuration des interfaces de Switch :**



❖ **Implémentation de 802.1x :**



❖ **Vérification de la configuration l'authentification 802.1x sur le Switch :**



V.5 Conclusion :

Dans notre étude, l'utilisation du protocole **802.1x** au sein du réseau local d'entreprise est prometteuse en terme de capacité de sécurisation des connexions.

Le protocole **802.1x** ne constitue pas une réponse absolue aux problématiques de connexion au réseau local mais s'avère être un outil simple et discret pour mieux contrôler l'usage du réseau.

Conclusion générale:

Dans ce mémoire, nous avons mis en œuvre une technique de sécurisation d'accès aux réseaux informatiques des entreprises, inter-entreprises afin de mieux garantir certains besoins de la sécurité : l'authentification, l'intégrité et la confidentialité des données échangées entre différents utilisateurs et d'éviter toute sorte de piratage informatique. Cette technique permet de contrôler l'accès physique aux équipements d'infrastructures réseaux en s'appuyant sur le protocole EAP pour le transport des informations d'identification en mode client/serveur, et un serveur d'identification RADIUS couplé avec à un Active Directory.

Après avoir installé et configuré Windows serveur 2003 (serveur DHCP, DNS, serveur RADIUS), Windows xp nous avons pu réaliser l'architecture de protocole 802.1x. Ensuite nous avons appliqué l'authentification au niveau d'un Switch Cisco à l'aide d'un simulateur réseau GNS3.

L'implémentation de 802.1x dans une infrastructure réseau est facile à réaliser et ne nécessite pas l'ajout d'un nouveau matériel au réseau, compte-tenu de la présence du serveur RADIUS, ce qui constitue l'un des avantages de la méthode. Quoi qu'elle ne permette pas d'assurer la sécurisation complète de tous les réseaux, prenant l'exemple des réseaux sans fil (faiblesse du protocole WEP).

En effet, la sécurité est proportionnelle aux différentes menaces, vulnérabilités qui augmentent au fur et à mesure, c'est ce qui fait de la sécurité informatiques un sujet très vastes et très important dans le domaine de la recherche, des améliorations peuvent être apportées sur notre travail, comme par exemple :

- Appliquer la méthode d'authentification 802.1x sur des routeurs pour mieux sécuriser l'accès inter réseaux.
- Appliquer la méthode d'authentification 802.1x sur des réseaux sans fil (Wifi).
- Utilisations d'un firewall pour une meilleure sécurisation.

Ce projet nous a permis d'améliorer nos connaissances dans le domaine des réseaux informatiques surtout ce qui concerne la sécurité. Nous avons compris l'importance des mécanismes de sécurité comme l'authentification, ces méthodes ainsi que ces protocoles.

Lors de la configuration du protocole 802.1x au niveau de l'authentificateur nous avons acquis beaucoup de connaissances sur le fonctionnement du matériels Cisco. Ainsi qu'on s'est familiarisé avec l'utilisation du simulateur GNS3 pour configurer les équipements Cisco (Switch, Retour, …).

Nous avons également eu beaucoup de plaisir à apprendre et nous familiariser avec le Windows server 2003 pour mieux gérer la sécurité notre architecture réseau.

Virtualisation de la topologie à configurer

Dans le but de simuler notre configuration réseau et de tester son fonctionnement ,nous avons opter pour la virtualisation de notre topologie qui est constituée des trois entités principales composant le protocole d'authentification 802.1X ,qui sont : le supplicant qui est une machine virtuelle cliente tournant sous le système d'exploitation Windows XP ,le Switch Cisco qui est configuré a l'aide d'un simulateur GNS3et le serveur Radius (dans notre cas service IAS) qui est configuré sur Windows Server2003, installé sur la deuxième machine virtuelle.

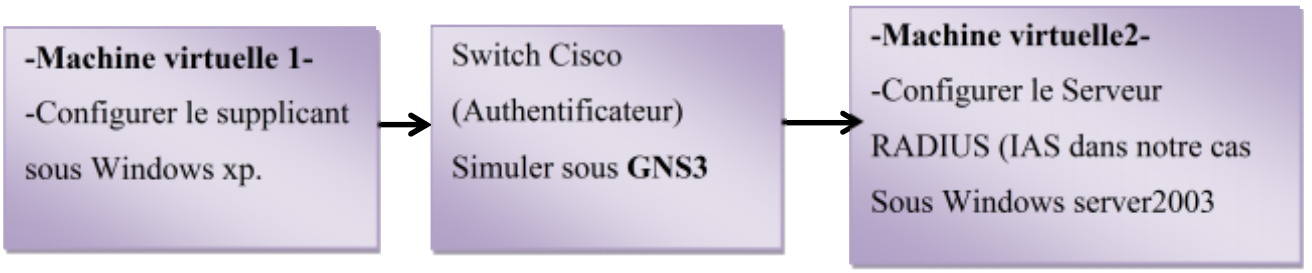


Figure 1: Schéma de virtualisation de la topologie

Et pour réaliser cette virtualisation nous avons utilisés l'outil de virtualisation Virtual PC de Microsoft.

Présentation de Virtual PC de Microsoft :

Microsoft Virtual PC est un logiciel qui permet d'exécuter simultanément plusieurs systèmes d'exploitation sur un même ordinateur. Il évite les configurations compliquées à chargement multiple dans les environnements où plusieurs systèmes d'exploitation sont nécessaires (que ce soit à cause d'applications anciennes incompatibles ou comme sécurité lors d'une migration). Les utilisateurs peuvent installer plusieurs systèmes d'exploitation hébergés dans des ordinateurs virtuels. **La figure** 2 montre Microsoft Windows® XP Professionnel avec deux ordinateurs virtuels ouverts : Windows NT® Workstation 4.0 et Windows 98. Virtual PC émule un ordinateur physique de façon la plus exacte possible afin que les applications ne fassent pas la différence entre l'ordinateur virtuel et un ordinateur physique. Au lieu d'installer des systèmes d'exploitation sur plusieurs ordinateurs coûteux ou de créer des installations lourdes à chargement multiple, nous pourrons installer les systèmes d'exploitation dans plusieurs ordinateurs virtuels, dans un même système physique. Les modifications apportées aux ordinateurs virtuels n'affectent pas l'ordinateur physique. Virtual

PC facilite l'utilisation de plusieurs systèmes d'exploitation en même temps, sur une même machine.

Virtual PC est une solution simple et économique qui répond aux besoins des utilisateurs qui doivent exécuter plusieurs systèmes d'exploitation en même temps sur un PC. En entreprise, il permet aux employés d'exécuter d'anciennes applications critiques sans ralentir l'évolution des postes de travail. Ainsi qu'avec Virtual PC Vous n'avez plus besoin d'acquérir un matériel additionnel uniquement pour prendre en charge les logiciels anciens qui ne fonctionnent pas sur une version récente de Windows. Il vous suffit de déployer Windows XP avec Virtual PC pour prendre en charge les utilisateurs qui doivent exécuter des applications incompatibles avec Windows XP.

Avec Virtual PC Vous pouvez ainsi créer autant de machines virtuelles que votre entreprise compte de poste de travail-type et les démarrer à la demande. Avec Virtual PC, les ingénieurs peuvent aussi tester des applications avec des délais plus courts dans une plus grande variété de configurations.

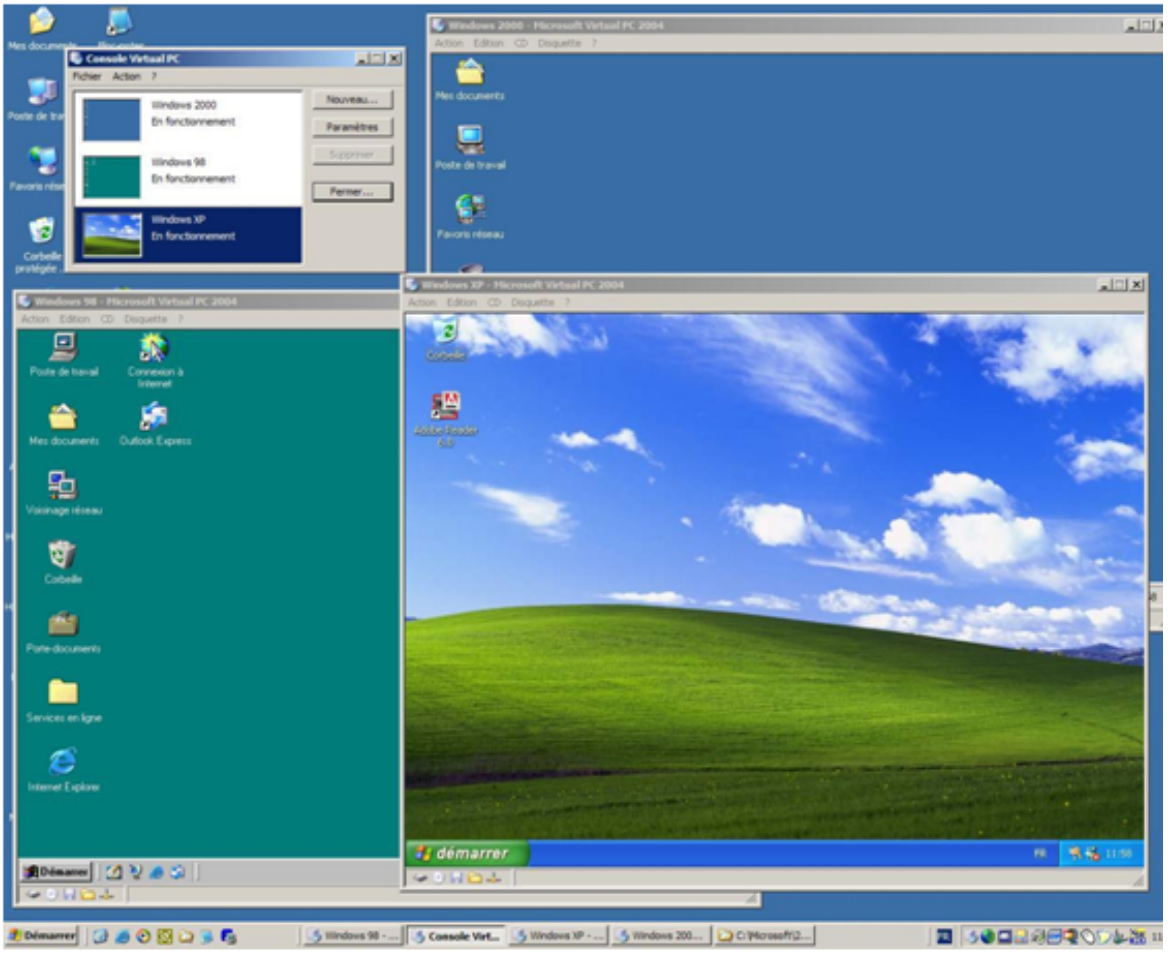


Figure 2 : Les systèmes d'exploitation hébergés Windows 98, Windows 2000 et Windows XP dans Windows XP.

Caractéristiques de Virtual PC :

Les avantages liés à l'utilisation de Virtual PC sont les suivants :

- **Simplicité de configuration :**

Les utilisateurs peuvent configurer des ordinateurs virtuels, ajouter ou supprimer de la mémoire et installer ou désinstaller des applications. Les utilisateurs peuvent créer une variété d'environnements et la facilité d'utilisation de Virtual PC permet de réduire les coûts liés à la formation. De même, le produit vous permet de contrôler la configuration de Virtual PC dans des environnements fermés.

- **Facilité d'installation :**

Virtual PC offre aux utilisateurs deux solutions pour ajouter de nouveaux systèmes d'exploitation hébergés. La première consiste à installer le système d'exploitation hébergé manuellement. La méthode est pratiquement identique à celle de l'installation du système d'exploitation sur un ordinateur physique. Dans les scénarios de migration, vous pouvez créer des configurations à l'avance, puis les déployer pour les utilisateurs.

- **Standardisation :**

Puisque le composant matériel de l'ordinateur virtuel ne change pas d'un ordinateur physique à l'autre, avec un seul ordinateur physique vous pouvez configurer et tester des mises à niveau et des installations sur des ordinateurs virtuels. Vous êtes ensuite en mesure de déployer dans toute votre entreprise une configuration standard à l'abri des bogues causés par les différences mineures entre plates-formes matérielles. Cette approche élimine les tests exhaustifs sur plusieurs ordinateurs.

- **Simplicité d'utilisation :**

Les utilisateurs peuvent passer d'un système d'exploitation à l'autre aussi facilement qu'ils changent d'application. Il leur suffit de cliquer sur la fenêtre contenant l'ordinateur virtuel. Ils peuvent arrêter des ordinateurs virtuels individuels pour qu'ils n'utilisent plus de cycles processeur sur l'ordinateur physique. Ils peuvent également sauvegarder des ordinateurs virtuels sur disque et les restaurer ultérieurement. Le processus de restauration prend normalement quelques secondes ce qui prend beaucoup moins de temps que de relancer le système d'exploitation hébergé. Les utilisateurs gèrent des ordinateurs virtuels en cours d'exécution, arrêtés et sauvegardés par le biais de la même interface utilisateur performante.

- **Intégration avec l'hôte :**

L'intégration facilite l'interopérabilité entre les systèmes d'exploitation hébergés et hôte. Par exemple, les utilisateurs peuvent faire des copier, coller, glisser et déposer entre le système hébergé et l'hôte. Virtual PC fournit des Compléments pour ordinateurs virtuels que vous installez dans le système d'exploitation hébergé pour bénéficier de cette fonctionnalité.

Chaque machine virtuelle agit comme un ordinateur autonome. Elle dispose de ses propres cartes son, vidéo et réseau, de son disque dur et de son propre processeur. Chaque machine virtuelle exécute aussi son propre système d'exploitation. Les utilisateurs peuvent installer et exécuter la plupart des systèmes d'exploitation x86 dans un ordinateur virtuel. Microsoft prend entièrement en charge les systèmes d'exploitation suivants pour l'exécution dans un ordinateur virtuel sur Virtual PC : Windows 95, Windows 98, Windows Me, Windows NT 4.0 Workstation, Windows 2000 Professionnel, Windows XP, MS-DOS, Linux. Les utilisateurs ont également la possibilité d'installer les systèmes d'exploitation **Windows Server**.

Disques durs virtuels :

Virtual PC prend en charge les disques durs virtuels de plusieurs façons qui allient puissance et flexibilité. Les utilisateurs peuvent associer plusieurs disques durs virtuels avec chaque machine virtuelle. Les types de disques pris en charge sont les suivants :

- **Disques durs virtuels à extension dynamique :**

Les disques durs virtuels sont un fichier unique que les utilisateurs créent sur le disque dur d'un ordinateur physique. Le fichier de disque dur virtuel s'étendra dynamiquement au fur et à mesure que les utilisateurs y écrivent des données. Ils utilisent initialement très peu d'espace, et s'étendent jusqu'à la taille maximale du disque.

- **Disques durs virtuels de taille fixe :**

Comme les disques durs virtuels à extension dynamique, les disques durs virtuels de taille fixe sont un fichier unique que les utilisateurs créent sur le disque dur d'un ordinateur physique. Le fichier a approximativement la même taille que le disque dur virtuel et il ne peut ni augmenter ni diminuer en taille. Par exemple, si un disque dur virtuel a une capacité de 2 Go, la taille du fichier de disque dur virtuel est de 2 Go.

Annexe B

Introduction :

L'objectif de cette partie est d'apprendre les différentes fonctionnalités des composants matériels et logiciels et la méthode de configuration des différentes matérielles Cisco (Switch, routeur et firewall).

Les commutateurs Cisco :

Définition :

Les commutateurs intelligents Cisco Catalyst, nouvelle famille de périphériques autonomes à configuration fixe, apportent aux postes de travail une connectivité FastEthernet et GigabitEthernet optimisent les services de LAN sur les réseaux d'entreprise. Ces caractéristiques sont :

- Sécurité du réseau assurée par une série de méthodes d'authentification, des technologies de cryptage des données et le contrôle des admissions sur le réseau basé sur les utilisateurs, les ports et les adresses MAC.
- Fonctionnalités intelligentes à la périphérie du réseau, par exemple des listes de Contrôle d'accès (ACL) élaborées et une sécurité optimisée

Figure : Les Switch CISCO

Configuration de Switch Cisco : On trois mode de configuration :

- Mode exécution : mode avec droit restreints (sw>).
- Mode privilégie ou enable (sw#).
- Mode configuration Sw (config).

enable : Passez du mode d'exécution utilisateur au mode d'exécution privilégié.
configure terminal : Passer du mode d'exécution privilégié au mode de configuration globale.
exit : pour descendre d'un niveau de commande
CTRL-Z ou end pour sortir du mode de configuration

Annexe B

Configuration de base d'un Switch:

Switch #configure terminal : Passer du mode d'exécution privilégié au mode de configuration globale.

Switch (config)#hostname sw1 : nommé le Switch.

Switch (config)#enable password : Configurer la commande enable password pour le passage en mode d'exécution privilégié.

Switch (config)#interface Vlan1 : Passer en mode de configuration d'interface pour l'interface du Vlan1.

Switch (config-if) # ip address 172.17.99.11 255.255.255.0 Configure l'adresse IP de l'interface.

Switch (config-if) # no shutdown: Activer l'interface.

Switch (config-if) # end: Repasser en mode d'exécution privilégié.

Switch (config)#interface fastethernet 0/1: Entrer dans l'interface pour affecter le réseau local virtuel.

Switch (config-if)#duplex auto: Configurer le mode birectionnel d'interface pour activer la configuration bidirectionnelle automatique.

Switch (config-if)#speed auto : Configurer la vitesse bidirectionnelle d'interface et activer la configuration de vitesse automatique.

Switch (config-if)#switchport mode access: Définir le mode d'appartenance du port à un réseau local virtuel.

Switch (config-if)# switchport acces vlan1 : Affecter le port à un réseau local virtuel **vlan1**.

Switch (config-if)#end : Repasser en mode d'exécution privilégié.

Switch (config)#Vlan 10 : créer un virtual local area network qui est Vlan10.

Switch (config-Vlan)# name V2 : nommé le Vlan 10

Switch (config)#ip default-gateway 172.17.99.1: Configurer la passerelle par défaut sur le Switch.

Switch (config)#end : Repasser en mode d'exécution privilégié.

Switch #copy running-config startup-config ou write memoiry: Enregistrer la configuration en cours dans la configuration de démarrage du commutateur.

Bibliographie

[1] : G.Pujolle, Eyrolles, « Initiation aux réseaux» IA 201, Vol 5, 2002.

[2] : Pillou , Jean François, « Tout sur le réseau informatique », IA 274, Vol 2.

[3] : C. Servin, Dunod, « Réseaux et Télécom », 2003.

[4] : GUY Pujolle, « Les réseaux », Edition 2008.

[5] : professeur Omar EL Kharki , « réseaux informatiques », cours, université Ibn Zohr, 2004.

[6] : Sécurité informatique principes et méthodes à l'usage des DSI, RSSI et administrateurs, 2éme édition, Bloch LAURENT, Christophe WOLFHUGEL.

[7] : Mr : MESSAOUI .Yacine, Mr : BOUFERRACHE .Younes, « conception et réalisation d'une application client/ serveur d'authentification, d'autorisation et d'Acounting dans un réseau sans fil cas : NAFTAL district Ouad Aissi », thèse d'ingénieur d'état en informatique, l'UMMTO, 2009.

[8] : Melle : LARABI. Drifa et Melle : YAHIAOUI .Karima, « sécurité des réseaux », thèse d'ingénieur d'état en informatique, l'UMMTO, 2005.

[9] : Mr MAMOU. Boussaad et Mr : TAYAB. Sofiane, « Implémentation du protocole d'authentification 802.1x à l'aide d'un serveur RADIUS », thèse d'ingénieur d'état en informatique, l'UMMTO, 2010.

[10]: Mr: HORRI. Mokhtar, Mr: AMAZIANE. Djamel, « Sécurité des réseaux mobiles multimédia (Ipv4, Ipv6) », thèse d'ingénieur d'état en Télécommunication, Institut de Télécommunication ORAN (ITO), 2007

[11] : Cours du module sécurité des réseaux informatiques de 2éme année Master en électronique option réseaux et télécommunications.

[12] : http://www.labo-microsoft.org/articles/win/ras2003/4/.

[13] : www.cisco.com.

[14] : http://fr.wikipedia.org/wiki/IEEE_802.1X.

[15] : http://www.commentcamarche.net/contents/wifi/wifi-802.1x.php3.

[16] :http://windows.microsoft.com/fr-FR/windows-vista/Enable-802-1X-authentication.

[17] :http://www.labo-microsoft.org/articles/network/pki-windows-server-2003/.

[18] : http://www.yopdf.biz/serveur-radius-pdf.html.

[19] : http://www.freeradius.org.

[20] : http://2003.jres.org/actes/paper.111.pdf.

[21] : http://www.youtube.com/watch?v=JNSY46EPiws&feature=related.